SUMÁRIO

SEMINÁRIO DE DIREITO ELETRÔNICO

25 de março de 2010

Manhã

25 de março de 2010

Tarde

26 de março de 2010

Manhã

26 de março de 2010

Tarde

ABERTURA

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Senhoras e senhores, bom dia a todos.

Iniciaremos o *Seminário de Direito Eletrônico*, uma iniciativa do Superior Tribunal de Justiça e do Instituto dos Magistrados do Distrito Federal (Imag-DF), que tem como proposta ministrar conhecimentos básicos e especializados sobre o Direito Eletrônico para o aprimoramento de servidores; ampliar a capacidade de interpretação das questões jurídicas surgidas no desempenho das funções exercidas; possibilitar a identificação das possíveis soluções jurídicas para os casos concretos; e, por fim, capacitar o participante à melhor utilização da terminologia técnico-científica do Direito nas atividades funcionais.

Convidamos o Presidente do Instituto dos Magistrados do Distrito Federal, Desembargador Valter Ferreira Xavier Filho, para o seu pronunciamento de abertura.

VALTER FERREIRA XAVIER FILHO
Desembargador e Presidente do
Instituto dos Magistrados do Distrito Federal

Bom dia a todos.

O Instituto dos Magistrados do Distrito Federal, no ano em que completa seu décimo aniversário, tem a honra de participar deste evento, em parceria com o Superior Tribunal de Justiça, que teve a iniciativa de capacitar seus servidores em uma área nova do Direito. Assim como, no final do século passado, iniciava-se o Direito Ambiental, hoje, podemos dizer que o Direito Eletrônico é uma realidade.

Preocupou-nos o tamanho do espaço deste auditório e a quantidade de pessoas a participar do evento, mas rendemo-nos à situação de que o mais importante é a qualidade, seja dos palestrantes, seja dos participantes e daquelas pessoas que vêm aqui para se informarem um pouco mais sobre esse ramo do Direito tão relevante na

atualidade.

Podemos verificar que, além de termos especialistas de renomado conhecimento na matéria, também temos, na qualidade de participantes, servidores que ocupam funções de relevo não apenas no Superior Tribunal de Justiça, mas no Supremo Tribunal Federal e nos demais tribunais superiores, pessoas que a Corte do Superior Tribunal de Justiça houve por bem permitir que participassem deste evento restrito, deste evento limitado, que, basicamente, visa ao aprimoramento e ao aperfeiçoamento dos servidores do próprio Superior Tribunal de Justiça.

Faremos um passeio pelo Direito Eletrônico, desde as ações fundamentais, desde as balizas constitucionais, passando pela responsabilidade civil, sem deixar de lado a parte fiscal e a tributária, o direito de propriedade, a questão contratual e, porque nem tudo são flores, a parte criminal, além da demonstração técnica do que acontece na área do Direito Eletrônico, que merece uma atenção especial daqueles que operam o Direito e visam uma sociedade que caminhe no sentido da perfeição, tanto de seus integrantes quanto de todo o contexto social.

Senhores, minhas palavras especiais são de agradecimento a todos aqueles que se dispuseram a participar destes trabalhos e, em especial, àquele que representa a primeira linha do Direito Eletrônico, nada mais nada menos, o Presidente do Instituto Brasileiro de Direito Eletrônico, que será o nosso primeiro palestrante, o Professor, o Doutor, o Mestre em Direito, José Carlos de Almeida Filho, a quem peço que assuma suas funções e me transforme em um ouvinte e em um dos seus alunos muito honrados.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Convidamos o Dr. José Carlos de Almeida Filho para a primeira palestra, com o tema *Processo Eletrônico*.

O Dr. José Carlos de Araújo Almeida Filho possui graduação em Direito pela Universidade Católica de Petrópolis e mestrado em Direito pela Universidade Gama Filho; é Professor de Direito Processual da Universidade Federal Fluminense e, também, Presidente do Instituto Brasileiro de Direito Eletrônico; é Professor convidado de pós-graduação da Universidade Católica de Minas Gerais e da Escola Superior de Advocacia de São Paulo; é autor da Obra *Processo Eletrônico e Teoria Geral do Processo Eletrônico*; é Diretor da Almeida Filho e Cesarino – Advogados Associados; possui experiência na área de Direito com ênfase em Direito Processual Civil, atuando principalmente nos temas: *Direito Eletrônico*, *Direito Processual Civil* e *Atos Processuais por Meio Eletrônico*.

PALESTRA I: PROCESSO ELETRÔNICO

JOSÉ CARLOS DE ARAÚJO ALMEIDA FILHO
Presidente do Instituto Brasileiro de Direito Eletrônico

Bom dia a todos.

Senhor Desembargador e Presidente do Imag, gostaria de iniciar a abertura dos trabalhos com esta palestra, que é de uma responsabilidade enorme e me deixa até um pouco assustado diante da qualidade que observamos, tanto no Superior Tribunal de Justiça quanto no Supremo Tribunal Federal, em termos de informatização.

Gostaria de começar com uma lembrança: a terceira edição da obra, para dizer que é fruto das primeiras intervenções do próprio Imag, por meio de algumas palestras proferidas para a Empresa Brasileira de Pesquisa Agropecuária (Embrapa), desde o início, vem sendo modificada. Digo isso porque observamos, com a informatização judicial no Brasil, desde as primeiras práticas e atos processuais, uma grande transformação. Volto a repetir que é de extrema dificuldade falar para uma plateia seleta como esta, porque os senhores, na realidade, têm muito mais a transmitir a nós que nós aos senhores.

A informatização, nos tribunais superiores, na realidade, vem sendo a grande ponta de lança da informatização judicial em todo o Brasil. Com a assinatura, pelos três Poderes, do 1º Pacto Republicano, que deu ênfase, posterior e simultaneamente, à Emenda Constitucional nº 45, houve a necessidade da informatização judicial.

Com o II Pacto Republicano houve a necessidade ou quase que a imposição pelo próprio Pacto de se inserir o juizado federal de forma totalmente eletrônica e, **pari passu**, ter, cada vez mais, todos os tribunais engajados na nova era, que é a da informatização judicial.

Gostaria apenas de, inicialmente, dar uma abrangência do que pretendo falar. Abordarei a informatização sob um novo foco, de trabalhá-la sob um novo prisma.

Até então, falávamos da informatização judicial como se fosse algo novo. A Academia e o Instituto Brasileiro de Direito Eletrônico vinham pesquisando o tema, pois possuem jovens e excelentes pesquisadores, como o Sr. Rony Vainzof, que tomará a palavra a seguir, companheiro do Sr. Renato Opice Blum, que também é uma das autoridades na área.

Faço um pequeno adendo para render uma homenagem ao Professor Renato, que não está presente, mas peço ao Professor Rony que transmita a ele estas palavras.

O Professor Renato, em 2001, ousou e lançou uma obra chamada *Direito Eletrônico*. Questionou-se: "Existe a disciplina Direito Eletrônico? Será que a nossa comunidade acadêmica está preparada para a ideia de um novo Direito, de um Direito das novas tecnologias, um Direito Eletrônico?" É um termo que soa de forma estranha para quem está acostumado com o Direito; que soa de forma chocante, porque o Direito não pode ser eletrônico. Mas ele é, na realidade, pois existe esse ramo do Direito e preferimos entender que a definição lançada em 2001, provavelmente fruto de pesquisas bem anteriores às do Professor Renato, seja a mais certa, que é exatamente Direito Eletrônico, e nada mais apropriado para um seminário como este levar tal título.

Farei apenas um pequeno retrospecto, porque, na realidade, ao falarmos em informatização judicial do processo, parece-nos algo muito novo, mas, na verdade, não é.

Os senhores, na realidade, são formadores de opinião: são assessores, estudantes, profissionais que lidam com os ministros, com os tribunais, que nos fazem, principalmente com as novas reformas do

processo, pensá-lo de uma forma, diria, até diferente, em determinados casos, pois o Superior Tribunal de Justiça possui decisões extremamente inovadoras em várias áreas do Direito.

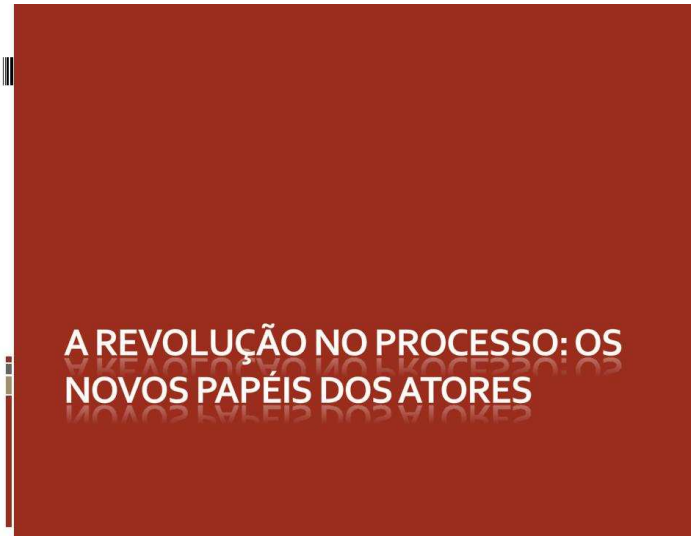
Como formadores de opinião, seria interessante voltarmos um pouco ao passado para analisarmos como a informatização veio num crescente no País para chegarmos aos dias de hoje e trabalharmos com a ideia de cibercultura; não é possível mais termos o processo estático como o imaginamos.

Gostaria de fazer mais um apêndice na palestra, antes de começar propriamente o tema da informatização, para dizer que estamos num ponto muito importante para que a informatização judicial seja, efetivamente, aplicada em todo Brasil, que é a construção de um novo Código de Processo Civil.

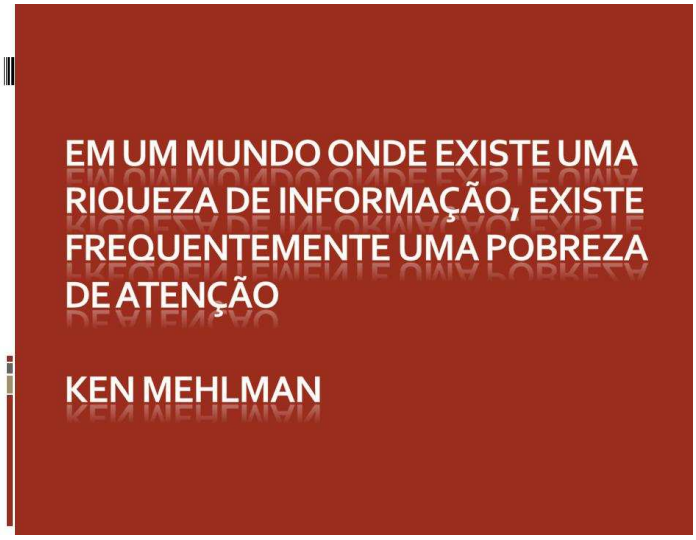
Temos a oportunidade, dentro do novo Código de Processo Civil, de lançarmos mão, cada vez mais, dos meios tecnológicos. Por exemplo, em termos de penhora, de leilão, de arrematação, o Professor José Miguel Garcia Medina teve a oportunidade de consultar o Instituto Brasileiro de Direito Processual (IBDP) – deixarei com os senhores o *blog*, no qual consta o texto completo, que é bastante interessante, do que seria um anteprojeto para a inserção dos meios eletrônicos na fase de execução.

Voltando ao passado, em 1991, ocorreu o que seria a primeira ideia de prática de ato processual por meio eletrônico.

Quando falo que estamos numa revolução no processo e que existem novos atores, os novos atores são todos.

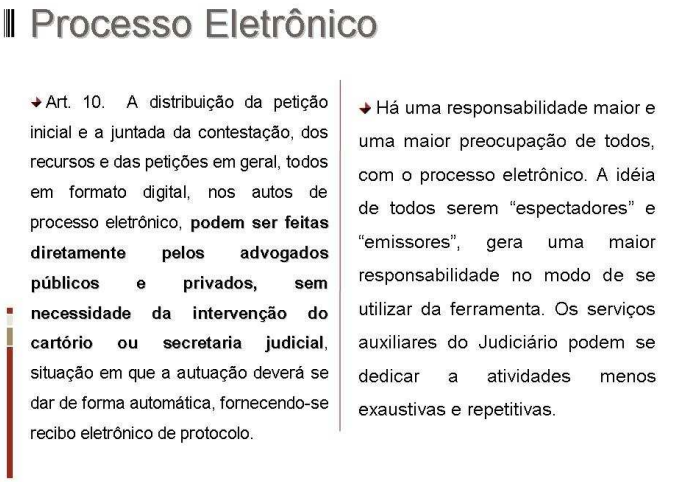


Existe um vídeo muito interessante na internet – deixarei meu *e-mail*, caso os senhores queiram que encaminhe esse vídeo –, tratando da revolução da mídia. Na realidade, é um vídeo muito mais voltado para agências de publicidade do que para o próprio Direito. Mas, se o concebermos na ideia do Direito como esse ramo do pensamento, como essa escola de construção social que é, nada fora da Sociologia e da Filosofia, veremos nesse vídeo a ideia do que seria o "prossumidor".



Na realidade, hoje, com o avanço da tecnologia, somos produtores e consumidores de informação ao mesmo tempo. A ideia do "prossumidor", do *prosumer*, é tratada nesse vídeo como um novo pensar dentro da cibercultura, em que há também novos atores no processo ou atores antigos com novos papéis. É repensar toda a estrutura arcaica para que, então, tenhamos uma modificação do pensamento dentro do próprio processo.

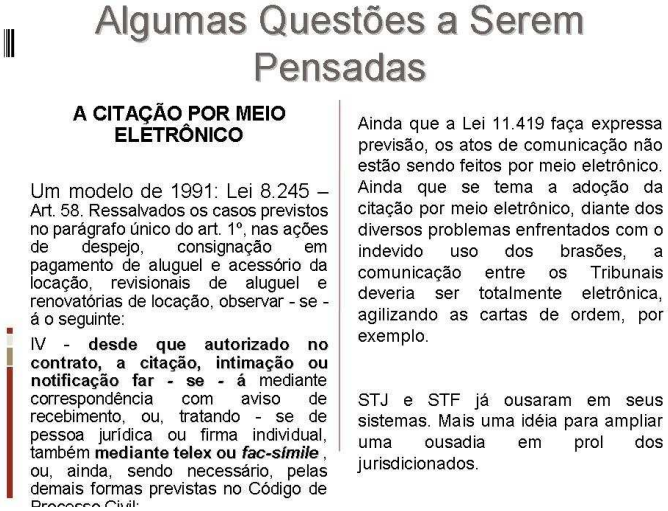
Admitir o processo eletrônico apenas como digitalização, transformação em banco de dados, transmissão *on line* de julgamentos, não é informatização. A informatização passa por um papel e nos faz uma provocação muito mais abrangente. Hoje, somos tanto advogados, servidores, ministros, desembargadores, juízes, quanto produtores e consumidores – utilizando um termo da mídia – daquele auto, físico, a que estávamos acostumados a manusear no cartório.



Atualmente, inserimos as peças, independentemente de intervenção cartorária, pois assim diz o art. 10 da Lei nº 11.419. Ainda que não funcione dessa forma, até porque não deve funcionar mesmo, e concordo que não deva funcionar, não deixa de ser o ato de produzir uma peça e inseri-la; apenas será manipulada no meio eletrônico, virtualmente, pois a inseri nos autos sem a intervenção cartorária.

Acredito que a ideia da inserção, independente de intervenção cartorária, tenha sido um pequeno erro legislativo, como a Lei nº 11.419, que é cheia de erros do início ao fim. Mas são erros, e são bastante justificáveis.

Voltando um pouco, como foi provocada a ideia de produzir e consumir os atos processuais, tratando numa linguagem em que se mistura o Direito com a mídia? Produzindo e consumindo esses atos processuais, voltamos ao passado, à Lei do Inquilinato, Lei nº 8.245, de 1991, pois, se a observarmos, poderemos ver que no art. 58 há a previsão expressa, desde que seja contratual, que a citação se fará mediante fax, um meio absolutamente inseguro. Mas, há previsão da norma, em 1991.



O que podemos admitir? É um meio eletrônico. É a prática de um ato processual de extremada importância, que é o chamamento do réu ao processo. Assim, em 1991, temos a primeira grande revolução do uso da tecnologia no Direito.

Em 1999, entra em vigor a Lei do Fax, Lei nº 9.800, de 1999, que, inclusive, foi alvo de inúmeras discussões no Superior Tribunal de Justiça, porque, à época, estávamos no auge da internet no Brasil, havíamos superado o *boom* de 1996 e a prática dos atos processuais nos tribunais superiores, até por dificuldade de locomoção de determinados estados até o Distrito Federal e por circunstâncias alheias à vontade do advogado ou da parte, pois muitos advogados encaminharam peças ao STJ por *e-mail*.

Mas a orientação jurisprudencial do STJ foi a de que o *e-mail* não seria similar ao fac-símile. Seria até interessante verificarmos, pois não tenho conhecimento de como está essa ideia, porque a Lei nº 11.419, de certa forma, acabou com ela, pois os atos processados por meio eletrônico, por disposição legal, são válidos. Então, todos os atos seriam válidos. Não vi uma modificação de pensamento no Superior Tribunal de

Justiça, até porque não há mais necessidade disso. A Lei do Fax, apesar de estar em vigor, parece-me que não tem mais tanta utilidade como nos anos 90.

CLÁUDIA AUSTREGÉSILO DE ATHAYDE BECK
Secretária dos Órgãos Julgadores

Ainda permanece o uso do fax para os processos físicos, mas, diante da digitalização, com certeza, tenderá a sumir a utilização do papel.

JOSÉ CARLOS DE ARAÚJO ALMEIDA FILHO

Acredito que ainda tenhamos muita discussão em relação ao *e-mail* e ao fax, pois penso que não se enviará *e-mail* sem se utilizar do portal do STJ.

CLÁUDIA AUSTREGÉSILO DE ATHAYDE BECK

Ainda permanece a discussão no âmbito das comunicações eletrônicas. Estamos em fase de conclusão de um convênio com o Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), por enquanto, no sentido de enviar as comunicações urgentes de forma *on line*, com a eliminação, portanto, da intermediação dos Correios e Telégrafos, que enviavam as comunicações por telegrama.

Discutiu-se – não sei se alguém da área de informática está presente para complementar o que estou dizendo –, a utilização do *e-mail*, mas, como a efetiva comprovação do seu recebimento seria frágil e geralmente, as comunicações urgentes envolvem a área criminal e outras questões de monta, como medidas cautelares e liminares em geral, concluiu-se que não era um meio seguro, por enquanto, para as comunicações urgentes de liminares.

JOSÉ CARLOS DE ARAÚJO ALMEIDA FILHO

Muito interessante. É bom ter essa visão.

Em relação aos atos de comunicação, há uma medida cautelar

tramitando nesta Casa, há um ano e meio, e, por dificuldade no cumprimento da carta de ordem, o réu só foi citado um ano e meio depois. Não é culpa do STJ nem do tribunal local, pois existe a figura dos Correios no meio, em que há desvios de malotes por perda, roubo e uma série de situações. Então, o que admitimos e é extremamente seguro, que é o físico, também podemos começar a duvidar.

A minha preocupação maior, enquanto advogado, ao produzir e encaminhar peças ao STJ, é a de que utilizar o fax é algo difícil, principalmente em determinadas matérias, pois é preciso complementar ou até emendar uma medida cautelar, por exemplo, e cumpro-a por meio do fax, mas são cem, duzentas páginas, e por *e-mail* seria muito mais fácil. Penso que, para nós, advogados, a ideia da Lei do Fax encontra-se um pouco superada. Gostaria de ver como o tribunal vai se manifestar diante disso, porque, na minha concepção, o *e-mail* é similar ao fax, sim, e até muito mais seguro.

Por haver tocado nesse ponto, faço um pequeno retrospecto.

Em 1939, quando se deu a inserção de um Código de Processo Civil nacionalmente, o grande berro que se deu à época foi o da utilização da datilografia. O uso da máquina de escrever seria um grande passo para a fraude nos processos, o que é interessante, porque se formos analisar, estamos no século XXI, desde o século XIX, a nossa grande preocupação sempre foi com a fraude. É uma mentalidade que deveríamos, inclusive, com o pensar de um novo processo, modificá-la, pois temos que pensar na boa-fé.

Os senhores estão acostumados a trabalhar com os ministros, assessorando-os, ou mesmo quem está advogando pode observar que existe, sim, a fraude e a má-fé, mas não é a tônica. A nossa política judiciária, a política jurídica, a nossa cultura política em termos de Judiciário, de atuação do advogado, é a do errado. Em vez de ingressarem no Tribunal com o peito aberto e falarem que são normais, chegam com medo, tendo que provar que são normais e honestos.

Diante de tanta coisa errada, diante do universo caótico que a nossa política se transformou, os ministros também se sentem constrangidos por receber os advogados, assim como os desembargadores e os juízes, porque a política que se criou é a da fraude. Temos essa ideia de comunicação.

O Professor Roney tratará de temas do Direito Constitucional, e é maravilhoso que o faça para que tenhamos a ideia do Direito Constitucional voltada para a área eletrônica. À frente, ao falar da responsabilidade civil, observarão, com muita tranquilidade, que a preocupação é sempre com a fraude, pois, como disse o Desembargador, nem tudo são flores, existem os crimes, mas é uma exceção. A norma, na realidade, não está aqui só para ordenar a média; só terá efetividade se houver uma quebra do que entendemos por ordenação mediana do nosso sistema.

Assim, quanto às questões sociológicas, o que me interessa muito na informatização vai além ou não muito além do Direito. A teoria alemã do Professor Gunther Teubner seria a do Direito como sistema autopoiético, que não admite a entrada nem a saída no nosso sistema.

A própria Sociologia trabalhará com a ideia e saída de informação, quer dizer, a produção da ideia e o seu consumo de uma forma autopoiética, que sobrevive por ela mesma, pois é algo circunferencial, não admitindo entrada nem saída; o direito vive dessa forma.

Voltando à ideia da fraude, em 1939, quando ocorreu o grande berro de que a utilização da datilografia provocaria fraude nos processos, admito já existir a fraude e que a nossa política é a da fraude, infelizmente.

Mas mudemos o pensamento. Em 1939, a grande discussão que havia em relação ao novo Código – época em que passamos a ter um Código nacional de processos não mais estaduais – é a de que o uso da caligrafia era extremamente seguro, mas está provado que não é. Se

observarem, seria até interessante por curiosidade e até faço um teste, 99% dos escritórios de contabilidade, senão 100%, e estou falando de uns dez anos atrás, porque agora as canetas fazem isso com muita tranquilidade, tinham como tônica a adoção da caneta tinteiro.

Todos os livros contábeis eram feitos com caneta tinteiro, para se ter uma ideia do porquê os processos também eram feitos com caneta tinteiro, por haver uma peculiaridade: com um pequeno bastão de cotonete e um pouco de água sanitária, passando por cima do que foi escrito, apaga-se, e a caneta tinteiro não machuca o papel. Gosto de fazer a comparação de não machucar o papel, porque a máquina de datilografia, por sua vez, machuca o papel.

Ao mostrarmos relutância em relação à informatização judicial, a primeira coisa que se diz é que vai ocorrer muita fraude. Em termos de informática, podem até me corrigir se estiver errado, esse "machucado" que se faz virtualmente é muito mais gritante do que o da própria máquina de escrever, pois existem os rastros dos *logs*, quer dizer, há uma série de requisitos que impedem a fraude.

Voltando ao passado, em 1991, temos a ideia da citação por fax, que é um meio eletrônico, daí a questão de se discutir se é similar ou não ao *e-mail* e admitido como meio eletrônico, visto que a forma de transmissão é feita por dado; a única diferença é que se terá um papel produzido com mais segurança, dependendo da espécie de papel ou do tipo de aparelho de fax, pois, se cair um copo de café no papel poderá apagar os dados, dependendo do material que se esteja utilizando.

Em 1999, foi criada a Lei do Fax e, em 2001, começou uma grande discussão que gerou algumas polêmicas. A primeira foi quanto à Lei nº 10.259, dos Juizados Especiais Cíveis e Criminais no âmbito da Justiça Federal, que, no seu art. 8º, há a previsão da prática de atos processuais por meio eletrônico, e esse mesmo artigo é o grande gerador do que temos hoje, que é a Lei nº 11.419, que poderíamos até entender o porquê dessa norma com diversos problemas. Admito que, de uma forma muito

tranquila, os tribunais podem resolver os problemas gerados pela Lei nº 11.419, visto que alguns artigos são totalmente desprezíveis, pois não há como serem aplicados efetivamente.

Da mesma forma, fazendo uma comparação, o Superior Tribunal de Justiça, desde 1999, diz que o *e-mail* não é similar ao *fax*, como, também, pode dizer, com muita tranquilidade, que não vai aceitar a citação ou intimação por meio do portal, como teria a ideia do art. 5º da Lei nº 11.419. É muito fácil, porque não tenho certeza de que a pessoa foi intimada, de que relevará o prazo, pois é melhor que não se aplique a norma.

Em 2001, temos a Lei nº 10.259, inserindo os juizados especiais federais e admitindo-se a prática dos atos processuais sem maior necessidade de um rigor em relação à utilização de uma ou outra chave de segurança em termos de informática.

Como a norma foi aplicada aos juizados especiais federais, a Associação dos Juízes Federais encaminhou, por meio da Comissão de Legislação Participativa da Câmara, o Projeto de Lei nº 5.828, um pouco tímido, com pouquíssimos artigos, fazendo previsão de práticas de atos processuais por meio eletrônico, sem qualquer segurança e sem a utilização de certificação digital.

Esse projeto tramitou durante longos anos na Câmara, depois, foi encaminhado ao Senado – contém uma emenda de redação absurda, uma péssima colcha de retalho, em que a emenda ficou muito pior que o soneto – e retornou à Câmara em 2006, para o Deputado José Eduardo Cardozo, Relator, que ficou muito preocupado com aquela norma, mas ouviu, o que é muito importante, os setores envolvidos na informatização judicial, como o Instituto Brasileiro de Direito Eletrônico e o Instituto Brasileiro de Direito Processual, com sede em Brasília, por meio do Procurador do Distrito Federal, Sr. Petrônio Calmon, além de ouvir o Instituto Nacional de Tecnologia da Informação (ITI), o Superior Tribunal de Justiça e o Supremo Tribunal Federal, à época, presidido pela Ministra

Ellen Gracie.

O Deputado José Eduardo Cardozo encontrou-se em um grande dilema: o Pacto Republicano, logo após a Emenda Constitucional nº 45, de 2004, impõe a informatização. Houve uma pressão da sociedade, pelo menos da comunidade jurídica, uma pressão efetiva e saudável em cima da Câmara dos Deputados para que a norma relativa à informatização judicial fosse sancionada. Havia a necessidade de uma tramitação não de urgência, por ser inconstitucional, porque não consta das previsões de tramitação com urgência, mas de simples urgência, pois o projeto estava, há 5 anos, tramitando na Casa. O que faz ele? Uma emenda de redação.

Daí, com toda a boa vontade do Deputado José Eduardo Cardozo, todos os atores convocados para ajudá-lo, tentaram, de alguma forma, elaborar uma emenda de redação à Lei nº 11.419, mas a emenda saiu pior que o soneto mais uma vez. Se observarem o art. 154, do CPC, verão que possui um parágrafo único, um § 1º e um § 2º. Acho que é o único País do mundo em que há uma lei com um parágrafo único seguido de dois parágrafos, ou seja, são três parágrafos num artigo em que há um parágrafo único.

Tal parágrafo único, na realidade, é um grande problema, porque, no ano de 2001, ao termos uma das grandes reformas do CPC, existiu a previsão **pari passu**, porque os projetos tramitaram, mais ou menos, na mesma época ou da lei dos juizados especiais ou da reforma do CPC.

Há a inserção no parágrafo único de tal possibilidade, porque, no art. 154, o que temos é o princípio da instrumentalidade das formas. O ato atingiu a sua finalidade e não há que ser declarado nulo.

Uma questão que é boa de ser pensada, para analisarmos a certificação do *site,* é a de imaginarmos se não estamos, efetivamente, tratando de processo, o que é importante que fique claro, pois a informatização judicial não é mera digitalização, não é mera tramitação por meio eletrônico e, sim, um novo pensar. Por isso a ideia de se

trabalhar com mídia quando estamos falando de informatização judicial e com uma maior humanização também com a utilização da informática.

A edição da Medida Provisória nº 2.200, de 2001, institui a Infraestrutura de Chaves Públicas, com mais duas reedições. A Medida Provisória nº 2.200, que insere a política de certificação digital, a Infraestrutura de Chaves Públicas, afirmando que só tem validade o documento, qualquer documento eletrônico, se assinado digitalmente, havendo a necessidade da certificação digital. Esse é um ponto também para deixar aqui pontuado.

O Superior Tribunal de Justiça, nesse ponto, foi mais adiante que o Supremo Tribunal Federal, pois desde o primeiro dia da instalação do portal do Superior Tribunal de Justiça foi exigida a certificação digital.

No Supremo Tribunal Federal, ocorreu a ideia do E-Proc, uma variação do Projudi, que é um processo que tramita no Conselho Nacional de Justiça. Gostaria de fazer um alerta, porque talvez os senhores não tenham percebido, de que a utilização do *login* e senha, se bem que no Supremo Tribunal Federal essa questão já está superada com um novo portal, simplesmente, coloca em xeque todos aqueles que participam do processo eletrônico no âmbito do CNJ.

Não há qualquer segurança na informação com a utilização de *login* e senha. Os dados dos magistrados que se encontram sob processo administrativo disciplinar, de alguma forma, estão, absolutamente, violados pela internet.

É fácil fazer a busca pelo nome de um magistrado e acessar o banco de dados do CNJ, porque não existe certificação digital. Com a necessidade da imposição da certificação digital com a Medida Provisória nº 2.200, o parágrafo único do art. 154 é vetado, exatamente, na mesma época em que se promulga a Lei nº 10.259, de 2001. Em questão de uma semana, há um veto presidencial: veta-se o parágrafo único, porque não é seguro – e não é mesmo. Foi até bom esse veto, porque provocou uma

discussão muito maior.

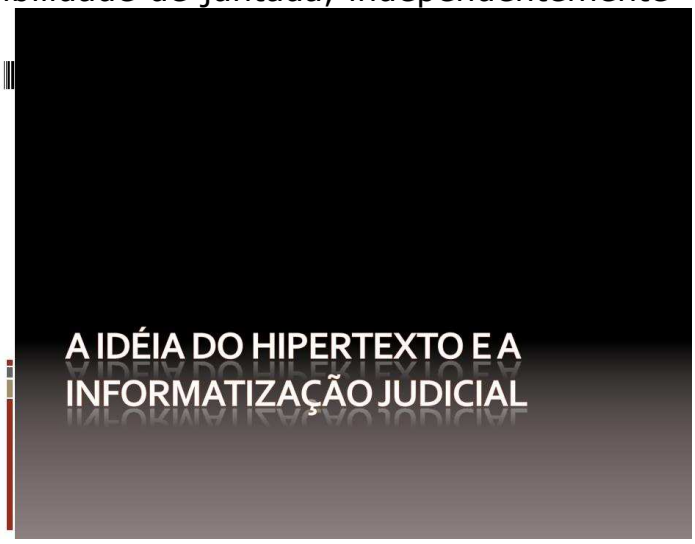
Então, seguindo o ano de 2001, temos algumas práticas de utilização de meios, como a possibilidade de acórdãos do STJ e do STF para efeito de paradigma e de manejo de recurso especial, e podemos, então, utilizar acórdãos retirados de *site* desses tribunais, indicando a data da publicação.

Mas não é essa, ainda, a ideia da informatização; o que temos, comumente, de informatização, como prática de ato processual é a possibilidade da citação por fax, a transmissão de peças, o cumprimento de prazo por meio do envio do fax e, em 2006, a Lei nº 11.419.

Como disse para os senhores, toda essa ideia da informatização provoca alguns pensamentos.

A partir de agora, desde o ingresso da Lei nº 11.419, com a redação do art. 10 – e sabemos que a mencionada Lei não funciona dessa forma e até seria muito interessante que não funcionasse –, temos uma responsabilidade maior de todos os atores do processo.

Existe até, dentro do art. 10, da Lei nº 11.419, uma interação maior entre o advogado e os tribunais; mas sabemos, pela prática que temos adotada hoje, no Superior Tribunal de Justiça e no Supremo Tribunal Federal, que a inexistência de intervenção do serventuário é algo absurdo. Desde o início, quando a Lei nº 11.419 veio a lume, houve uma crítica enorme em relação à possibilidade de juntada, independentemente da intervenção cartorária.



O que visualizo, em termos de não intervenção, seria a ideia do hipertexto, trabalhada por Pierre Lévy numa ideia de cibercultura.

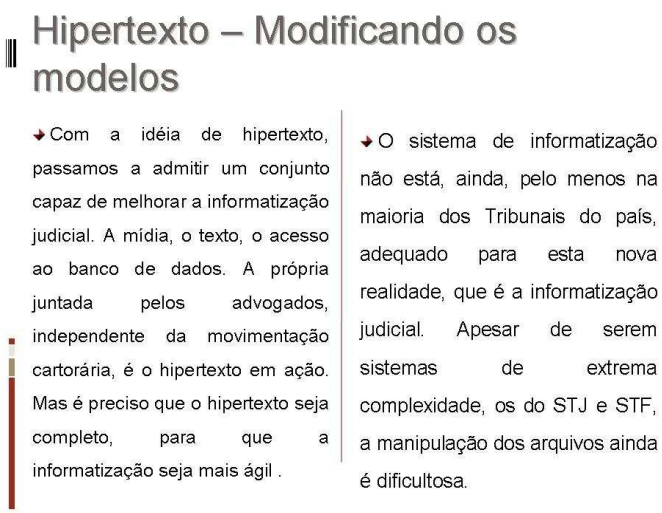
Na realidade, gostaria de fazer uma provocação para

os senhores levarem aos ministros, de como podemos ter o acesso ao portal do STJ, à tramitação dos atos processuais com base no hipertexto, de como podemos ter uma informatização mais humana.

Farei novamente um pequeno adendo, fugindo um pouco do tema processo e voltando à Sociologia aplicada nesse novo modo de pensar o processo; atualmente, temos uma humanização excessiva com a adoção dos meios eletrônicos. No primeiro momento, a grande repulsa à Lei nº 11.419, a grande repulsa à prática de ato processual por meio eletrônico foi por parte dos serventuários. A ideia é clara e não a critico, visto que foi importante demais tanto a manifestação quanto a preocupação dos serventuários.

Se existe a possibilidade de o advogado inserir nos autos o que bem entender, se existe a possibilidade de um feito tramitar absolutamente por meio eletrônico, qual seria o papel? O papel não muda. O que admito é o que modifica a responsabilidade. Sobre outro aspecto, se tenho uma aceleração – não vamos ter a Lei nº 11.419 como uma panaceia para a solução dos problemas judiciários, porque não conseguiremos –, na realidade, não podemos culpar o Judiciário pelo retardo, pois não é culpa dele, mas de uma política jurídica que existe, de que é interessante ganhar tempo, uma política jurídica que o Superior Tribunal de Justiça é um Tribunal de terceira instância, da mesma forma que o Supremo Tribunal Federal. O que podemos observar, na prática, é que 99% dos recursos manejados às Cortes Superiores transformaram-nas em cortes revisoras das cortes estaduais, o que é um absurdo.

Como a filosofia vem sendo cada vez mais adotada e, principalmente, quando falamos em informática, em informatização, é muito importante que tenhamos a ideia filosófica construída dentro de nós, pois estamos num momento muito importante de repensar o processo. A ideia da informatização, do Direito Eletrônico não é a de falar que é uma mera ferramenta a ser inserida no Judiciário, mas, sim, de repensar o processo como um todo.



Fazendo um paradoxo muito interessante entre Nietzsche, em sua obra *Humano, Demasiado Humano*, e a área da informática seria "humano, demasiadamente eletrônico e o eletrônico demasiadamente humano" para chegar a trabalhar o humano como eletrônico, ideia de Pierre Lévy de hipertexto, avançar na cibercultura, pois a informatização judicial não foge da ideia de cibercultura. Temos uma nova cultura, um novo modo de pensar, inclusive, da informatização judicial.

Não sei se os senhores observaram, mas não gosto de usar o termo processo eletrônico, porque acho que essa norma não seja processual, é uma norma procedimental do início ao fim, com ampliação de princípios processuais, uma norma de natureza procedimental.

Os Professores Wambier[1], Teresa e Medina[2] vão um pouco mais além ao dizerem que a norma não é só procedimental, mas é uma meta procedimental.

São questões acadêmicas interessantes de serem analisadas, pois, se admitirmos a Lei nº 11.419 como procedimento, teremos a possibilidade de legislação concorrente, por força do art. 24 da Constituição; então, os estados poderiam legislar sobre procedimentos.

---

[1] **Luiz Rodrigues Wambier** é um jurista brasileiro, professor de Direito Processual Civil. Doutor em Direito Processual Civil pela PUC-SP. Formado pela Universidade Estadual de Ponta Grossa-PR em 1977; é Mestre em Direito pela Universidade Estadual de Londrina em 1989 e Doutor em Direito pela Pontifícia Universidade Católica de São Paulo em 1996. Professor no curso de mestrado em direito da Universidade de Ribeirão Preto(UNAERP); Professor no curso de especialização em direito processual civil da Pontifícia Universidade Católica de São Paulo; Ex-professor dos cursos de graduação, especialização e mestrado da Universidade Estadual de Ponta Grossa. (Wikipédia)

[2] Breves comentários à nova sistemática processual civil 2 – 2ª edição, em co-autoria com Teresa Arruda Alvim Wambier e José Miguel Garcia Medina Católica de São Paulo; Ex-professor dos cursos de graduação, especialização e mestrado da Universidade Estadual de Ponta Grossa. (Wikipédia)

Temos, no Supremo Tribunal Federal, a Declaração de Inconstitucionalidade da norma paulista, que determina o interrogatório *on line* do preso, que é a videoconferência. Há uma ação declaratória de inconstitucionalidade, porque há uma lei estadual paulista permitindo a videoconferência.

Retornando à ideia do humano e do eletrônico, tenho uma ampliação da responsabilidade de todos esses atores no processo e a possibilidade de os serventuários trabalharem – essa é a nossa visão de fora e seria interessante que os senhores se manifestassem também –, dia a dia, com essa informatização, ou seja, nós produzindo de um lado e os senhores, produzindo de outro. A nossa produção, o nosso pensamento em relação à ideia de como funciona o processo dentro dos tribunais e a ideia do serventuário é empírica. O retorno dos senhores, para mim, é muito importante.

Temos a idéia da humanização da seguinte forma: com a possibilidade de encaminhamento, porque, inserindo a peça processual no sistema, diminuo o tempo de trabalho para a verificação daquele material, e, com isso, tenho mais qualidade de vida e mais servidores saudáveis. Não tenho nada a ver com isso, mas é uma matéria interessante, pois seria bom que os tribunais se preocupassem com isso, que seria a questão, também, de se ter uma meta de trabalho com um intervalo de 2 horas.

Falo isso, como se eu fizesse, mas não o faço, como se trabalhasse na informática durante 8 horas, fazendo um intervalo – as questões de saúde ocupacional devem ser analisadas também, porque vamos utilizar, cada vez, mais a ferramenta, cada vez mais o computador.

Se a postura está inadequada, em virtude do uso do computador, e você já está olhando de lado, mas acabei de operar a coluna cervical por causa disso, porque as posturas vão ficando, cada vez mais tortas, provocando uma questão de humanização em relação ao trabalho – mas não é a minha tônica, não entendo nada de direito do trabalho e posso me

manifestar.

A ideia de humanização do Poder Judiciário é a de dar mais tempo a esses servidores para que dêem mais atenção aos senhores ministros, mais atenção para a produção de melhores mecanismos e ferramentas para a produção de decisões cada vez mais próximas da realidade.

A sensação que me dá é a de que a informatização nos trouxe essa humanização. Estou mais próximo do meu colega, estou mais próximo do ministro, não preciso ficar folheando, furando, costurando; em termos de agilização prática de trabalho, tenho uma grande economia e, em virtude dela, a utilização da ferramenta eletrônica e uma humanização maior, pois, se maior o contato, maior a possibilidade de o assessor produzir mais trabalho em relação ao que vier a ser julgado. Há uma pesquisa maior do que vem sendo discutido a esse respeito, e veremos essa ideia com as passagens de Pierre Lévy em *Tecnologias da Inteligência* e outras obras, como a *Cibercultura*, que admito de fundamental importância.

Fazendo um pequeno aparte, desde que as pesquisas na área da informatização começaram a ser produzidas por um grupo, começamos a perceber que, cada vez mais, se tornaram necessárias as pesquisas nos campos da Filosofia e da Sociologia.

Se os senhores observarem, pois não é preciso fugir dos tribunais, a internet, a comunicação que se faz por meio dos canais de comunicação eletrônica modificou totalmente a linguagem. A palavra "abraços" se escreve "abs", o que significa freio. Existem tantas formas de linguagem modificadas com o uso da internet que precisaremos começar a pensar a comunicação dentro do meio eletrônico, principalmente no que está relacionado ao processo.

Daí, a questão de se reforçar a Lei nº 11.419, pois, apesar de a matéria tratada nela ser procedimental, existe um novo processo a ser construído. As normas procedimentais não estão alheias ao sistema processual, muito pelo contrário, há um engajamento dentro da política

judiciária.

Como estamos tratando essas ideias no campo da Sociologia e da Filosofia, é importante agilizar o trabalho relacionado ao processo – e aqui vem a ideia de provocar os tribunais para se modificarem um pouco –, que, na realidade, é algo muito mais informático do que propriamente jurídico, mas, se formos analisar a modificação do hipertexto, por meio dele, poderemos ter uma informatização mais ágil e eficiente.

O hipertexto seria de uma forma simplista, a conjugação de uma nova linguagem, pois, atualmente, existe uma nova fala e uma nova escrita. Há grupos de pesquisadores que vêm trabalhando, cada vez mais, acredito que até com certo exagero, na modificação total da escrita em virtude da informatização judicial.

O hipertexto é a conjunção da produção dos novos atores no processo, dos antigos atores ou da modificação do papel desses atores no processo, a elaboração de textos, a elaboração de decisão, a elaboração de um tramitar do processo e a inserção disso tudo num banco de dados.

O banco de dados é algo interessante em termos de adoção do hipertexto, porque vai trabalhar com todas as linguagens que temos conhecimento, e, a partir da adoção dessas linguagens, teremos a indexação delas em bancos de dados, que já são bastante conhecidos.

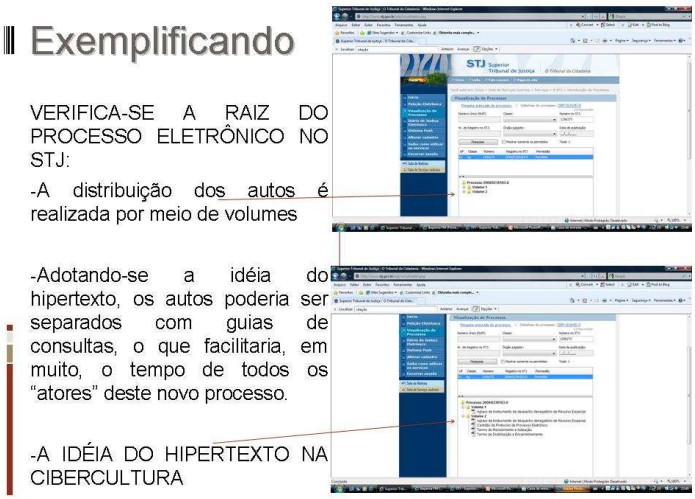
Pierre Lévy faz uma remissão, para que entendamos o hipertexto, bastante interessante: antes dos anos 70, a *Apple* cria um aparelho, pois não existia computador da forma como imaginamos hoje, o que é óbvio. Antes, comprava-se um computar por peça, comprava-se um processador muito frágil, e montava-se o computador. Em determinado momento, um empresário disse que não queria ficar montando as peças, pois queria a peça montada.

A partir dos anos 70, temos a criação do *Apple I*, depois do *Apple II*, mas a grande revolução que se tem em termos de hipertexto, naquela época – porque até os anos 70, mais ou menos, essas máquinas pessoais,

toda vez que se abria o computador tinha que programá-lo e reprogramá-lo –, foi da fita cassete.

A maioria dos presentes talvez nem se lembre dessas fitas, pois se gravava utilizando-se um gravador, e a imagem era exibida no monitor de TV. A ideia do hipertexto foi a de modificar a forma de pensar a ferramenta, modificar a forma de gravar o dado da ferramenta e mantê-lo de alguma forma preservado.

Ao acessar o *site* do Superior Tribunal de Justiça, por exemplo, e desejar fazer a análise de um feito que tramita na Casa, o que se vê, na realidade, é apenas a modificação do papel para o meio eletrônico. Teremos o Volume I e o Volume II. Realmente, essa é uma provocação que, para nós, seria ótima e acredito que para os senhores também, mas uma grande provocação.



Se tenho os Volumes I e II, no Volume I, em termos de matéria de informatização judicial, não vejo nada de diferente do que existe nos autos físicos. Na última capa, tenho um resumo completo do que consta nos autos, como um agravo de instrumento na folha tal; nesse caso, nem as folhas tenho.

Qual seria a ideia do hipertexto? Contarei para os senhores uma experiência muito interessante, realizada no Tribunal Regional do Trabalho da 9ª Região, em Curitiba, em que todas as audiências são gravadas. Ao voltarmos à ideia de humanização, por meio da utilização dos canais eletrônicos na informatização judicial, a grande discussão que se está travando por lá, que admito deva ser superada em breve, e seria muito interessante que o Superior Tribunal de Justiça a eliminasse, é quanto à

necessidade de degravação do conteúdo produzido em multimídia.

Existe uma audiência inteira gravada e filmada. Por meio de um sistema criado pelo Tribunal Regional do Trabalho da 9ª Região, os autos, na forma eletrônica, além de estarem disponíveis os Volumes I e II, há uma indexação, e continuo avançando na ideia do hipertexto, que, inclusive, é do Pierre Lévy.

O que ganho com a indexação? Num *click*, em um segundo, posso procurar, por exemplo, a peça de um advogado. Daí vem a ideia da humanização e, inclusive, admito, da melhoria de todo o sistema judiciário nacional, que pode ser provocado pelo Superior Tribunal de Justiça ou pelo Supremo Tribunal Federal, que são os Tribunais que já possuem uma informatização, uma ideia de autos cem por cento eletrônicos.

A ideia do hipertexto, da indexação da informação, é muito ágil. Se colocar "razões de apelação", com um *click* no *mouse*, verei a página. Ainda preservamos a cultura do folhear, que também é interessante, porque, ao folhear, sempre tenho a ideia de que, em algum momento, li algo. Na indexação, posso continuar tendo a mesma sensação de que, em algum lugar, em algum momento, li algo, que pode ser de extrema importância no momento de proferir um voto, assim como para o advogado utilizar-se de embargos de declaração, porque aquela parte não foi lida pelo Ministro ou, no caso, pelos assessores. Então, teríamos omissões nas decisões por uma deficiência na tramitação dessas peças por meio eletrônico.

O Tribunal Regional do Trabalho da 9ª Região criou um sistema muito interessante, chamado Fidelis, que contém a gravação da audiência, e, nesses termos, é interessante, porque existe um paradoxo, mas, em termos de informatização judicial, podemos até questionar se necessitamos relativizar, ou não, o princípio da publicidade. Admito que sim, e poderemos falar rapidamente sobre isso.

O Tribunal Regional do Trabalho da 9ª Região possui um sistema

de indexação, **pari passu**, de todos os atos produzidos, que seriam escritos em meio eletrônico, e a oralidade, que seria a ampliação do princípio da oralidade, porque sabemos que esse princípio abrange ainda o princípio da adstrição, o princípio da identidade física do juiz. Há uma série de princípios abarcados pelo princípio da oralidade, todavia, uma ampliação dos efeitos desse princípio com a informatização judicial traz, exatamente, a ideia de levar o juiz de 2º Grau à humanização do que se vê na audiência.

Aconteceu uma situação bastante interessante no Tribunal, porque era uma preocupação minha, de questionar os desembargadores a respeito da gravação das audiências. A quantidade de recursos que sobe hoje ao Tribunal Regional do Trabalho da 9ª Região, por cerceamento de defesa, por indeferimento de perguntas, é muito menor. É infinitamente menor do que ocorria nos autos físicos, e por quê? A ideia da gravação é muito interessante, pois, numa audiência de primeira instância, existe um combate emocional enorme – o processo é pura emoção. Existem conflitos em resistência e necessitamos da autoridade do Estado para solucioná-los. A grande beleza do processo é a pacificação da sociedade por meio da resolução dos conflitos.

Tenho um ambiente de extrema complexidade e extremamente belicoso, tanto que, Piero Calamandrei[3], ao tratar do processo, no século XIX, afirmava: "Há armas no processo". Quer dizer, temos que ter paridade de armas e o processo não pode ser visto dessa forma, apesar de não podermos tapar os olhos.

Na audiência de primeira instância, quando temos esse ambiente extremamente belicoso e as emoções à flor da pele, duas situações podem ocorrer e não podemos "tapar o sol com a peneira" em hipótese alguma:

[3] **Piero Calamandrei** (Florença, 21 de abril de 1889 — Florença, 27 de setembro de 1956) foi um jornalista, jurista, político e docente universitário italiano. (Wikipédia)
Junto com Francesco Carnelutti e Enrico Redenti foi um dos principais inspiradores do Código de Processo Civil de 1940, onde trabalhou na formulação legislativa e no ensino fundamental da escola de Giuseppe Chiovenda. Foi impedido de continuar na carreira de professor universitário por não subscrever uma carta de submissão ao «duce» que era uma exigência na época. Nomeado Reitor da Universidade de Florença em 26 de julho de 1943, até 8 de setembro, pois foi atingido por um mandado de prisão, somente exerceu efetivamente o seu mandato em setembro 1944, com a libertação em Florença, em outubro de 1947.

uma, evidentemente, é o magistrado, que já está cansado de ver aquela situação e, por algum motivo – o termo que vou utilizar é meramente jurídico –, ser arbitrário, indeferir questões e, de alguma forma, se comportar com poder – é óbvio que esse poder do magistrado existe –, mas, com poder além dos poderes, além da barreira do abuso de poder, impedindo também exaltações do advogado. A humanização, a busca da verdade real é uma questão interessante.

A verdade no Direito é dupla: se tenho uma verdade, tenho uma verdade real e tenho uma verdade formal. Mas a verdade é una. O certo é que nunca chegaremos à verdade, mas fica-se muito próximo do que seja verdadeiro. Por quê? Há um comportamento excessivo de todos aqueles atores que estão participando quando há a gravação.

Ao afirmarmos que há uma ampliação dos efeitos do princípio da oralidade, e o procedimento eletrônico tem essa questão bastante interessante, vários dos efeitos dos nossos princípios processuais são elevados imensamente com a utilização dos atos processuais, uns, extremamente saudáveis, outros, extremamente prejudiciais.

Quando esse feito chega ao tribunal, chega absolutamente indexado. A ideia de hipertexto é completa e a audiência é toda separada. Se, em determinado momento, o acórdão for embargado, porque o desembargador não apreciou a questão das horas extras, por exemplo, poderá clicar no indexador – seria muito interessante se a gestão de informática dos tribunais conseguisse fazer isso, para que os ministros que estão envolvidos com a informatização, os desembargadores e os juízes que as analisassem, tivessem uma aceleração – "hora extra" e terá a indexação do que foi produzido na audiência. Ocorrerá o princípio da adstrição: o pedido com a defesa, as testemunhas de defesa, as do reclamante, as do reclamado e ouvirá, com precisão, somente o trecho em que ele fala das horas extras.

Temos, com a utilização de meios eletrônicos no processo, uma ampliação enorme da questão da humanização.

Como falei da ampliação de princípios, há um, em específico, que me causa um pouco de pavor: o princípio da publicidade. Por exemplo, sabemos que é uma garantia, um direito fundamental e existe exatamente em contraposição ao tribunal de exceção. Lembra-me um pouco aquelas cenas que podemos visualizar com tranquilidade quando se lê Foucault[4], em *Vigiar e Punir*, onde temos, na Idade Média, os tribunais de exceção, a Inquisição, um julgamento cem por cento não publicizado, mas, para dar satisfação à sociedade, tenho cem por cento de publicização da pena.

Veio à minha mente uma imagem interessante, fazendo uma analogia com o que Foucault trata em sua obra: "Quando vou esquartejar o cidadão, tenho cavalos tracionando o homem. Em determinados momentos, sou obrigado até a cortá-lo com machados, porque o corpo precisa ser separado. Aquele pobre coitado que foi condenado precisa ser esquartejado para que o crime dele seja limpo".

Terei uma publicização e uma agressividade enorme na aplicação da pena, porque o processo tramitou de forma cem por cento sigilosa, mas a pena tem que ser pública.

O que observamos, hoje, em termos de informatização, o que é um grande perigo – vamos analisar depois a certificação do *site*, que é a ampliação não digo do princípio, mas dos efeitos do princípio da publicidade –, é que sabemos que os atos processuais devem ser públicos, pois é uma determinação e uma garantia

[4] **Michel Foucault** (Poitiers, 15 de outubro de 1926 — Paris, 25 de junho de 1984) foi um importante filósofo e professor da cátedra de História dos Sistemas de Pensamento no Collège de France desde 1970 a 1984. Todo o seu trabalho foi desenvolvido em uma arqueologia do saber filosófico, da experiência literária e da análise do discurso. Seu trabalho também se concentrou sobre a relação entre poder e governamentalidade, e das práticas de subjetivação.

constitucional, o que inibe os tribunais de exceção, impede que haja um feito sem que o amplo direito de defesa seja devidamente respeitado, mas, por outro lado, temos uma publicização excessiva, que pode ser extremamente prejudicial.

Houve, recentemente, uma decisão inédita do Tribunal do Rio de Janeiro, numa discussão em sede de **habeas corpus** – e venho provocando essa discussão há uns quatro anos, mais ou menos –, num feito em que, em tese, há a prática de um crime próprio de informática, que seria a interceptação de dado telemático. Todos os atos desse feito, sem exceção, estão disponíveis na internet: os depoimentos das testemunhas estão disponíveis na íntegra, assim como os atos processuais, as ocorrências das audiências. A questão que se colocou ao Tribunal foi a seguinte: há publicização excessiva, porque o princípio da publicidade não dá o direito de, se sou réu numa demanda, o autor inserir isso na Folha de S. Paulo, no Correio Brasiliense ou em outro jornal todos os dias. Ele não tem esse direito.

Existem outros princípios em contraposição ao princípio da publicidade, ou seja, não tenho direitos fundamentais absolutos, segundo falava a Professora Ada Pellegrini com muita tranquilidade.

Vou trabalhar com uma ponderação de princípios bastante interessante. Se há uma ampliação do princípio da publicidade – e, agora, temos uma publicização excessivamente alargada, que é a do *You Tube* e da TV Justiça –, temos que começar a pensar se, efetivamente, temos o direito de ter essa ampliação, de levar a cabo a ampliação dos efeitos do princípio da publicidade.

Antes, admitindo-se os autos físicos, dirigia-me ao C

artório para ter a noção do que estaria acontecendo em determinado processo se houvesse interesse próprio. Aqui, me interessa, num sistema, se o réu está em estado de inocência, não vou dizer que é presunção de inocência, mas ele é inocente e, se é inocente, o estado é de

inocência, não é presunção de inocência. O Estado é quem tem que provar que ele é réu, que ele é culpado.

O processo penal tem que ser garantístico e, ao tratarmos da informatização, estamos tratando de todos os processos: penal, do trabalho e civil. A questão tem que ser analisada por esse aspecto.

Óbvio, se há testemunhas de acusação, que morrem de raiva do réu e falam barbaridade dele, está na internet, mas há também testemunhas que falam maravilhas do réu. A questão é a seguinte: a íntegra dos depoimentos na internet interfere na próxima testemunha que virá depor em juízo? Interfere. Na prática, interfere. É uma publicização excessiva.

Se há uma audiência gravada, por exemplo, e ela aparece no Y*ou Tube*, é uma discussão que venho debatendo e até encaminhei um pedido à Ouvidoria do Supremo Tribunal Federal para entender como funciona essa publicização excessiva dos julgamentos, pois, sinceramente, não sei se é bom, se é válido, se estaremos diante de uma demonstração da importância dos nossos tribunais superiores ou se estaremos, de alguma forma, trabalhando dentro da ideia de cibercultura com a banalização do nosso sistema.

Se tivermos, com a informatização, e digo que isso não é a informatização do processo, mas uma ampliação extremada com o uso dos canais eletrônicos, em que vamos inserindo, cada vez mais, informações e caímos, volta e meia, no hipertexto, na ideia de cibercultura, que pensar na publicização excessiva, devemos pensar com muito cuidado: se estamos dando efetiva publicidade aos nossos julgamentos ou se estamos banalizando as nossas cortes, o que é muito complicado.

De certa forma, colocamos todos esses novos atores num novo procedimento eletrônico, de ampliação dos efeitos dos princípios; estamos colocando todos eles em xeque, o que não é saudável, sob a minha ótica,

e gostaria até de ouvir as ressalvas, não admito como saudável para a corte, para o jurisdicionado. Temo, inclusive, como aconteceu no passado, quando se fizeram bolões na internet, um grande *Big Brother*, dizendo-se, por exemplo, que o Ministro A é mais simpático do que o Ministro B, porque bateram boca em determinada sessão do plenário.

Não entendo, não consigo visualizar essa publicização excessiva como algo saudável à nossa sociedade, à comunidade jurídica. Os nossos tribunais têm que ser cada vez mais preservados e menos colocados à disposição da mídia, para termos como resultado a preservação do ambiente, a preservação da garantia e a preservação da efetividade das decisões.

Admito que seja importante pensarmos sobre o seguinte: se inserirem o meu nome completo no Tribunal de Justiça do Estado do Rio de Janeiro, na Vara de Família – o que digo com muita tranquilidade, porque foi um feito muito tranquilo –, verão que sou separado consensualmente. A quem interessa isso? A quem interessa fazer uma busca na internet e saber que sou separado judicialmente?

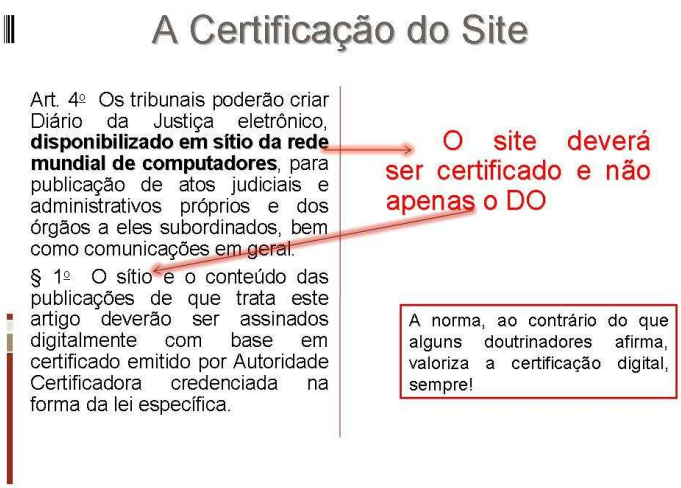
CLÁUDIA AUSTREGÉSILO DE ATHAYDE BECK

Seria considerado um segredo de justiça.

JOSÉ CARLOS DE ARAÚJO ALMEIDA FILHO

Exatamente. Pela própria norma do art. 155 do Código de Processo Civil, essa informação jamais poderia estar lá. Mas, não me incomoda nem um pouco, pois não existe, absolutamente, nada de mais, a não ser uma sentença homologatória.

Continuando: imaginemos que, mesmo com o art. 155, com a impossibilidade de determinados atos se tornarem públicos, um feito que tramita na vara criminal por agressão oriunda de violência doméstica e uma ação de separação extremamente complexa em virtude daquele feito criminal, todos os atos processuais se encontram, sem exceção, disponíveis na internet.



Surgirá uma questão interessante, que quero provocar, futuramente, no entendimento do Superior Tribunal de Justiça. Não sei no que dará, mas há casos em que se torna necessário este pensamento: se analisarmos o art. 4º da Lei nº 11.419, verificaremos que o Diário da Justiça eletrônico será assinado digitalmente, mas o *site* do Tribunal também tem que ser certificado, não apenas o Diário Oficial. Não sei se a minha leitura está equivocada, mas parece-me que no § 1º haja a necessidade da certificação digital do próprio *site* do Tribunal.

Questiono o seguinte: se tenho um feito que tramita da forma como falei, um feito de direito de família no Juizado Especial Criminal de Violência Doméstica, com base na Lei Maria da Penha, e for totalmente violado, totalmente divulgado?

Vou mais longe – é óbvio que sabemos que essa não é a regra, mas o que confirma a regra é exatamente a exceção –, alguns casos são bastante marcantes, como o caso que ocorreu em São Paulo, há muitos anos, de um casal de japoneses acusado de pedofilia, de aliciamento de menores em uma creche. Hoje, moram debaixo de um viaduto. A publicização excessiva acabou com a vida desses senhores.

Imaginemos, por exemplo, uma senhora que se autolesiona – o que não é difícil, o que confirmará a regra é, exatamente, a exceção, que seria a autolesão dessa pessoa –, porque não suporta mais a vida em comum, além de vários motivos, mas não importa qual, e resolve de alguma forma representar contra o seu companheiro e ajuizar uma ação de separação. Se não tenho um *site* certificado digitalmente, há a possibilidade de qualquer um que o acesse navegar como se navega em

qualquer página da internet e fazer tal verificação.

Na cibercultura passeamos de um lado para outro na internet. Se, de repente, há dez anos não vejo determinada pessoa e quero procurá-la, no *Facebook*, no *Twitter*, não importa, e me corresponder com ela; posso até namorá-la, descobrir o grande amor da minha infância e encontrá-la. Mas ela poderá dizer: "Nossa! Aquele cara é um agressor, não vou chegar perto dele". Daí a uns dez anos, é comprovado que houve uma autolesão, então, destruí vidas, tive uma série de problemas, e, mais, violei a própria norma.

A questão que pergunto é: se um *site* não é certificado digitalmente e minhas informações processuais tramitam dentro dele sem a utilização da certificação digital – e, aqui, vou utilizar o E-Proc do Conselho Nacional de Justiça –, e suponhamos que eu esteja defendendo com muita tranquilidade um magistrado num procedimento administrativo dentro do CNJ, o acesso ao *site* do CNJ é somente por *login* e senha, mas, de alguma forma, deixa-se vazar, sem inserir qualquer informação, por algum motivo, no *Google*.

A busca do nome do magistrado no *Google*, num processo administrativo sigiloso em que o *site* não seja certificado digitalmente, o manejo de mandado de segurança para coibir o ato do CNJ, do conselheiro, seria o da nulidade absoluta de todos os atos processuais praticados. Não tenho como aplicar, pelo menos, nesse primeiro momento, e venho defendendo isso, porque, em termos de informatização e para que tenhamos uma política de informatização com a adoção da Infraestrutura de Chaves Públicas, com a adoção da Medida Provisória n° 2.200, não consigo ver na hipótese do art.4°, a utilização do princípio da instrumentalidade das formas.

O ato atingiu a sua finalidade, mas a que preço essa finalidade foi atingida? Sempre faço questão de dizer que a ampliação dos efeitos dos princípios é que devem ser analisadas nessa nova era em que estamos tratando da informatização judicial.

Qual o preço que se paga por não se ter uma certificação digital? Por exemplo, o que já é público e notório no caso do Arruda, suponhamos que, por algum motivo, por quebra de sigilo bancário ou por quebra de sigilo fiscal, tenhamos que tramitar com aquele feito em segredo de justiça – esqueçamos o *site* do Superior Tribunal de Justiça, porque é certificado, enquanto que o do Supremo Tribunal Federal e o do Conselho Nacional de Justiça não são – suponhamos que, pela inexistência da certificação digital do *site,* a defesa consiga anular todo um processo, porque está totalmente violado na internet, por inobservância ao art.4°. O princípio da instrumentalidade das formas não poderá ser aplicado nesse momento. Deve ser totalmente mitigado, assim como a ampliação dos efeitos do princípio da publicidade também não deve ser aplicada nesse momento.

A excessiva publicização dos atos processuais vem causando cada vez mais problemas. Futuramente, uma teoria de nulidade, que pode vir sendo construída em termos de atos processuais por meio eletrônico, poderá vir a invalidar uma série de processos e transformar a informatização judicial no contraponto do que desejamos, que é exatamente a aceleração do Judiciário, o que não é panaceia.

A ideia da informatização é exatamente a de uma aceleração do andamento dos feitos. Se não tivermos essa preocupação premente e a adotarmos como vêm adotando diversos tribunais no País, afirmando que não há necessidade da certificação digital, que não tem motivo, é frescura, é muito caro, terei uma nulidade absoluta, que pode ser gerada no feito, como, por exemplo, se os senhores me perguntarem qual foi o meu objetivo ao arguir o princípio da publicidade e a necessidade de se extrair todas as peças dos autos, todos os andamentos dos autos da internet no caso criminal de interceptação da telemática? Pode-se perguntar, porque temos de analisar a cabeça do advogado e a cabeça do Poder Judiciário: toda a decisão tem um efeito secundário que, às vezes, não se apresenta de imediato?

Se o Tribunal de Justiça do Rio de Janeiro diz que o ato da autoridade coatora, do juízo de primeira instância, é ilegal, o da inserção de todo o andamento do feito na internet, qual o próximo passo? Petição simples arguindo a nulidade do feito desde o interrogatório do réu. Olhem os efeitos da decisão, por uma inobservância.

CLÁUDIA AUSTREGÉSILO DE ATHAYDE BECK

Quanto às partes, há a questão das indenizações por dano moral.

JOSÉ CARLOS DE ARAÚJO ALMEIDA FILHO

Com certeza. Ótima colocação.

Ontem, quando estava a caminho para pegar o vôo e conversava com o motorista, disse-me que havia ganhado uma indenização de 300 mil reais contra a seguradora, porque não pagaram o carro dele. Perguntou para mim: "Será que a penhora *on line* já foi deferida?" É interessante, porque as partes estão, cada vez mais, familiarizando-se com os novos termos e estamos utilizando termos menos pesados. Disse a ele: espere só um minuto, que verifico se a juíza deferiu o bloqueio ou não; pedi que me informasse o nome das partes e o nome do advogado. Constava que ele ganhou 300 mil reais, em uma indenização pequena para sequestro.

Mas suponhamos um caso que está deixando o município do Rio de Janeiro à flor da pele, que é o da Carvalho Hosken contra o município; feito que já veio para o Superior Tribunal de Justiça, foi anulado, voltou para o Rio de Janeiro e está tramitando. Na semana passada, houve uma discussão absurda; nesta semana, foi adiado de novo, há pedido de vista; refere-se a 1 bilhão de reais em discussão.

Questiono-me se é interessante que a população tenha conhecimento de que determinada empresa – se bem que para a Carvalho Hosken, não é nada – ganhou um milhão de reais. Se fosse o dono dela, coitados dos meus filhos, seriam vítimas de sequestro ou de outros atos.

Então, devemos analisar com extrema cautela essa ampliação dos

efeitos que temos com a ideia de hipertexto, de uma cibercultura.

É muito bom este Seminário, visto que a primeira palestra, na realidade, é sobre um tema que os senhores estão cansados de conhecer, da informatização judicial, pois trabalham com ele todos os dias. Mas admito, pelo que conheço do Professor Rony e do Professor Marco Antônio, que farão suas apresentações, e tenho quase certeza de que os senhores sairão daqui com muitas dúvidas – o que é muito bom.

A ideia de dúvida é filosófica, porque a partir da dúvida irei fazer a construção de um todo. É muito importante que se provoque nos senhores, que estão no dia a dia dessa luta, para que pensemos, no Direito Eletrônico, que já é um fato. A informatização judicial deve ser pensada sob outros enfoques, porque, até agora, o que tenho visto muito é que todos os autos foram digitalizados, são questões ainda um pouco burocráticas em termos de informatização. Mas a informatização, passada a fase burocrática, deve ser concebida como uma nova forma de pensar o processo, uma nova forma de pensarmos os princípios processuais.

A possibilidade de uma construção de novas nulidades processuais com a adoção dos meios eletrônicos, confesso aos senhores, vem sendo objeto de pesquisa minha. Para nós, advogados, é excelente, e digo isso porque, anular um determinado feito em que sabemos que não há a menor possibilidade de se chegar ao fim com uma vitória, para o nosso cliente, é bom. Que não achem absurdo, porque é o papel do advogado, óbvio, desde que não atinja a má-fé.

O processo, em seu formalismo, nos conduzirá, de repente, a uma extinção ou a uma nulidade absoluta, até em um caso criminal, no qual, depois de 5 anos de uma instrução criminal, depois de 4 anos discutindo-se a publicização excessiva dos atos, com uma decisão que afirma que é ilegal a inserção de todos aqueles atos, questiono: como a audiência foi bipartida várias vezes, o fato de haver o depoimento das testemunhas ali será que não provocou a modificação do pensamento de outras testemunhas? Isso não teria prejudicado a instrução? Até que ponto esse

prejuízo causado à defesa, em um processo penal garantístico, não me daria o direito de pleitear a nulidade de todo o feito a partir do interrogatório?

É uma decisão muito complicada do Tribunal do Rio, porque se fala que aquilo é ilegal, todos os atos processuais são ilegais, e há uma nulidade absoluta que não tenho como adotar o princípio da instrumentalidade das formas, em hipótese alguma.

Gostaria muito mais de provocá-los do que, efetivamente, trazer algo de novo, porque o novo quem está trazendo são os senhores.

Com a informatização judicial, ocorreu um fato bastante interessante, pois estamos acostumados a ver que, em determinados movimentos dentro do Direito, quem começa a provocação geralmente é a academia, geralmente é o advogado com alguma tese que se cria, a discussão sobre algum plano econômico e a construção jurisprudencial vem sendo formada em cima de provocações acadêmicas ou provocações dos advogados; uma modificação de papel pareceu-me muito interessante: quem acreditou na informatização judicial, desde a sua origem, desde 1991, foi o Poder Judiciário; quem foi retrógrado, nesse ponto, foi a instituição que sempre lutou pela democratização neste País, a Ordem dos Advogados do Brasil.

Não sei se é do conhecimento dos senhores, mas a Ordem dos Advogados do Brasil ajuizou três Ações Diretas de Inconstitucionalidade contra a Lei nº 11.419, em que uma delas permeia o ridículo – ingressamos como **amicus curiae** e, quando falo que permeia o ridículo não estou falando nada além do que defendemos como **amicus curiae** na Ação Direta de Inconstitucionalidade –, é contra a portaria do Tribunal de Justiça de Sergipe, que inaugura o Diário da Justiça eletrônico.

Ajuizada a Ação Declaratória de Inconstitucionalidade contra o Tribunal de Justiça de Sergipe, uma semana depois do ajuizamento dessa, a Ordem dos Advogados do Brasil comparece ao Supremo Tribunal

Federal, em sessão solene, e assina um ato com a Sra. Ministra Ellen Gracie para a implantação do Diário da Justiça eletrônica no âmbito do Supremo Tribunal Federal.

Quando digo que a ação permeia o ridículo é porque, para o Tribunal de Justiça de Sergipe, já que a Ordem não foi convidada para o ato solene de assinatura da portaria, é inconstitucional. Mas, uma semana depois, a Sra. Ministra Ellen Gracie assina, com muita propriedade, o Diário da Justiça eletrônico, e a OAB encontra-se presente para a assinatura.

A segunda Ação Direta de Inconstitucionalidade da OAB foi contra o parágrafo único, com dois parágrafos, do art. 154, uma ação inócua.

Finalmente, a Ação Direta de Inconstitucionalidade nº 3.880, se não me engano, cujo Relator era o Sr. Ministro Ricardo Lewandowski, contra todos os dispositivos da Lei nº 11.419. O grande argumento da Ordem dos Advogados do Brasil contra a informatização judicial diz:

Art. 133 da Constituição: "O advogado é indispensável à administração da justiça (...)". Ótimo. O fato de eu ter de me cadastrar no Supremo Tribunal Federal ou ao STJ, viola o art. 133 da Constituição. Mas viola em que sentido? Qual a violação que tenho? Fico imaginando o seguinte: para ingressar no STJ e fazer uma sustentação oral, preciso passar na portaria, identificar-me, o que é muito saudável. Passo pela portaria e me apresento: sou advogado, vou fazer sustentação oral, ando pelo prédio com o crachá, não há problema algum. Onde está a inconstitucionalidade de eu andar pelo mesmo tribunal, de forma eletrônica? É o mesmo tipo de credenciamento. Em hipótese alguma, viola o art. 133 da Constituição.

Admito que essas três Ações Diretas de Inconstitucionalidade perderam o seu objeto há muito tempo. Peticionamos, recentemente, e pedimos a perda de objeto. Em um dos nossos encontros, em algum evento, à época, o Doutor Cezar Britto disse-me: "Por que não desiste

dessas ações? Se o Supremo Tribunal Federal está com o seu processo eletrônico todo implantado, você acha que o Tribunal vai dizer que é inconstitucional uma norma, na qual também não vejo nenhum ponto de inconstitucionalidade?"

Não sei até que ponto chegou a ideia do que é inconstitucional. O que temos de inconstitucional na Lei nº 11.419? Absolutamente nada. Talvez, com muito esforço, e realmente seria um problema a ser enfrentado, seria do art. 18, que permite que os tribunais regulamentem a Lei.

Ocorreu um erro de redação enorme, porque não foi o que o legislador quis dizer. O que o legislador quis dizer foi o seguinte: não é a lei que será regulamentada, são os atos administrativos do tribunal, saber que tipo de programa utilizará, como a prática de um ato pode vir a ser praticada, mas a Lei, em si, não vai ser regulamentada pelo Poder Judiciário; senão, seria uma loucura, cada tribunal regulamentando a Lei nº 11.419. Daí, a inconstitucionalidade seria flagrante. Muito saudável seria, simplesmente, suprimir o art. 18, que não causaria problema algum. Os tribunais, por regimento interno, podem, com muita tranquilidade, resolver a questão.

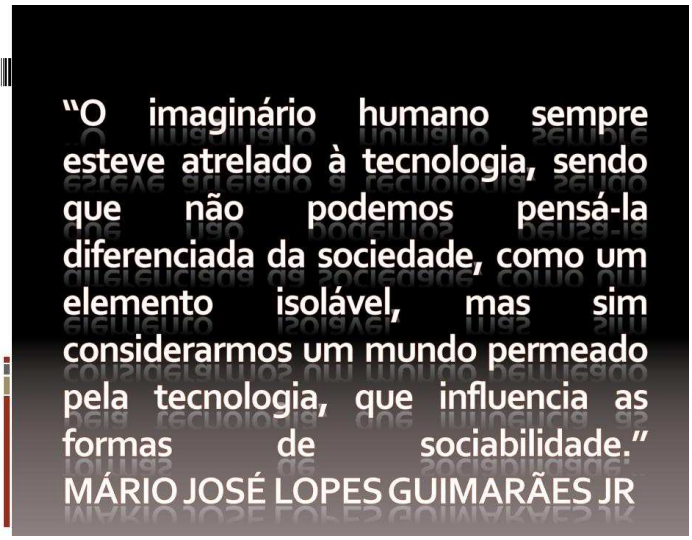
Para finalizar, gostaria de falar da questão da comunicação dos atos processuais para com os tribunais.

Ao adotarmos a ideia do hipertexto precisamos entendê-la, porque o nosso imaginário está atrelado à tecnologia e formos analisá-la não é somente a utilização da informática, na idade da pedra tecnológica não foi descobrir a roda, o fogo e por aí afora, mas vivenciamos uma sociedade não apenas de comunicação, porque temos uma sociedade de comunicação e de informação desde que o mundo é mundo, temos uma ampliação dessa sociedade da comunicação com a invenção da prensa, e uma ampliação exagerada, agora, com a internet e dos meios de comunicação eletrônicos que temos a sociedade da informação tecnológica.

Dentro da ideia de sociedade da informação tecnológica, podemos ter uma construção de um *site*, são portais noventa por cento seguros, com a utilização de certificação digital, para a comunicação dos atos processuais com os tribunais. Seria, inclusive, o primeiro passo dado pelos tribunais superiores a criação de uma intranet com acesso de todos os tribunais, em que se encaminharia uma mensagem, ou por sistemas interligados.

Por exemplo, se os senhores receberem um torpedo enviado por mim, o telefone apitará ou vibrará, fará algum barulho. É tão simples trabalhar com isso, que os tribunais poderão ter um sistema nacional integrado. A partir dessa integração, haverá um canal de comunicação que dará um alerta de que ali existe uma carta de ordem, que não precisa ser encaminhada por *e-mail*, porque, quando se afirma que não há a origem da recepção, no fax tenho muito menos origem de comprovação do recebimento.

Poderá acontecer, como ocorreu outro dia, ao receber um fax, no meu escritório, pois saía em branco; recebia outro, e saía em branco, era a tinta que havia acabado, pois tinta também acaba. Quer dizer, dizia-se que o fax estava com defeito, mas o defeito estava no cartucho, que havia acabado.



O que tenho com a tramitação? O fax, para mim, não oferece segurança alguma, mas sistemas adotados pelo tribunal dentro de portais, com certificação digital, é uma ideia que tem que ser cada vez mais valorizada, e fico feliz pelo STJ ter sido o primeiro Tribunal no País a exigir a certificação digital; o Supremo não exigia e passou a exigir. Agora, só falta o CNJ aderir à ideia da certificação digital para que todos os tribunais

do País sigam o exemplo das nossas Cortes Superiores, porque há a possibilidade de comunicação desses atos processuais – cumprimento de precatório, por exemplo, e emissão de carta de ordem –, pois não podemos ter uma cautelar que leve um ano e meio com um ministro, reiterando o ofício para que confirme se a parte foi citada, porque, às vezes, não interessa a ela também, ser citada; não interessa ao réu ser citado em uma medida cautelar que concedeu efeito suspensivo ao recurso especial, ou que não tenha concedido efeito suspensivo, e ficará aguardando o réu por quanto tempo? Noventa e nove por cento das cautelares perdem o objeto, então não há necessidade, não há por que perder o objeto; os dois podem ser julgados simultaneamente – a medida cautelar e o recurso –, não há problema.

Dentro da ideia do hipertexto, dentro do trabalho de construção do que temos e pelo que vi, até agora, não será muito difícil pegar o que já está construído e, simplesmente, adequar, adaptar para um sistema de comunicação dos atos processuais nacionalmente.

Encerrando, coloco-me à disposição caso os senhores queiram fazer alguma pergunta; o importante é provocar cada vez mais essa nossa vontade da construção de um direito. O Direito é muito vivo e, quando admitimos que a tecnologia é mais viva do que o Direito, começamos a ver que o Direito está tão vivo quanto ou, se duvidar, até mais.

O que nos deixa muito felizes é saber que existe a preocupação de todos esses novos atores na informatização judicial, não de brincar com ferramentas, não de ficar navegando nos *sites* e ter uma apresentação para o mundo de algo, mas o que verificamos, o que podemos observar é que a informatização, no Brasil, está fazendo o que nós, brasileiros, temos de melhor.

Acredito que sejamos um povo cem por cento humano, o que é próprio do brasileiro e, com a informatização, temos condição de, cada vez mais, sermos mais e mais humanos, quer dizer, temos a informática para trabalhar para nós como ferramenta; o processo, como um todo,

para pacificar essa nossa sociedade conturbada, e, de alguma forma, tentarmos fazer com que essas decisões sejam um pouco mais rápidas.

Temos um paradoxo no processo, que é o da efetividade e, em prol dessa efetividade, dessa imediatidade da decisão, acabamos, muitas vezes, sacrificando a qualidade. Não se trata de uma crítica, mas uma constatação – ninguém consegue ser rápido e muito bom ao mesmo tempo, pois é muito difícil.

Com a ideia do hipertexto, da nova informatização, pelo menos assim, visualizo, e gostaria que fosse uma visualização, um movimento que tivéssemos dessa humanização para a pacificação e que tenhamos um tempo razoável de duração do processo, com qualidade. Admito que, com a informatização judicial, consigamos isso e, inclusive, minimizaremos os grandes conflitos que temos na sociedade, muitos provocados por culpa dos advogados.

Agradeço aos senhores, ao Instituto dos Magistrados, Desembargador Valter, a todos os presentes. Gostaria de finalizar agradecendo pela humanização que esses tribunais têm levado a todo o Brasil; a importância que têm é reconhecida e sabida por todos. Quem pesquisa o dia a dia sabe que só conseguimos ter a construção de um processo, a construção de uma ideia de pacificação não com os ministros apenas, não com os advogados, não com os serventuários, mas somos um todo.

Queria dizer que somos um todo e é uma pena até que, na lei, haja a obrigatoriedade de todos se tratarem com urbanidade, pois considero isso uma pena, porque a urbanidade deveria ser natural, própria do ser humano e não precisaria constar em lei para que fôssemos tão

humanos.

Agradeço a todos por essa humanização que têm trazido para o País e saibam que os nossos tribunais, hoje, são referência no mundo em termos de informatização judicial.

Muito obrigado.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

O Seminário de Direito Eletrônico é uma iniciativa do Centro de Estudos Superiores do Instituto dos Magistrados do Distrito Federal (Imag-DF).

Para ministrar a Palestra, com o tema *Questões Constitucionais em Direito Eletrônico*, convidamos o palestrante, Dr. Rony Vainzof, sócio do Opice Blum Advogados Associados; graduado pela Faculdade de Direito da Universidade Presbiteriana Mackenzie e Pós-Graduado em Direito Processual Penal pela mesma Universidade; Coordenador, Assistente e Professor do MBA em Direito Eletrônico da Escola Paulista de Direito – EPD; Professor convidado da Fundação Getúlio Vargas e da Universidade Presbiteriana Mackenzie nos cursos de Pós-Graduação em Direito Digital e das Telecomunicações, bem como Computação Forense; professor das Faculdades FIAP, IBTA, UNIGRAN, UNICID E UNISA e do Instituto Paulista de Educação Continuada; é, ainda, Vice-Presidente do Conselho Superior de Tecnologia da Informação da Federação do Comércio do Estado de São Paulo e Vice-Presidente do Comitê de Direito da Tecnologia da Câmara Americana do Comércio – Amcham.

Com a palavra o Dr. Rony Vainzof.

PALESTRA II: QUESTÕES CONSTITUCIONAIS EM DIREITO ELETRÔNICO

RONY VAINZOF
Professor do MBA em Direito Eletrônico da Escola Paulista de Direito

Bom dia a todos.

É um grande prazer estar com os senhores nesta manhã e, aliás, é um grande orgulho estar no Superior Tribunal de Justiça para ministrar duas palestras, uma sobre Questões Constitucionais e outra sobre Direito Civil, relacionadas à minha área de atuação e à minha paixão propriamente dita que é o Direito Eletrônico.

Agradeço o convite do Instituto dos Magistrados e do Superior Tribunal de Justiça em poder passar um pouco da minha experiência relacionada a essa minha área de atuação.

Realmente é fantástico um seminário como este, poder contar com palestrantes renomados na área do Direito Eletrônico, como o Dr. José Carlos Almeida Filho, que acabou de ministrar uma palestra a respeito do Processo Eletrônico, inclusive indico o livro dele de Processo Eletrônico como bibliografia na Universidade Presbiteriana Mackenzie, onde ministro aula sobre Processo Eletrônico. Os senhores terão um pouco da prática relacionada às novas tecnologias, o que é bastante interessante. Amanhã, os senhores participarão da Palestra VII, Crimes Eletrônicos, com o Dr. Augusto Rossini, Promotor de Justiça, um grande amigo e excepcional palestrante e profissional, e também da Palestra V, Propriedade Imaterial do Direito Eletrônico.

Desejo que continuem tendo um ótimo Seminário.

Fiquei bastante curioso com a indagação do Dr. José Carlos acerca do que aparece primeiro quando se pesquisa no *Google* sobre a palavra mentiroso. Espero que não seja nenhum de nós aqui. Tenho a obrigação de ministrar uma boa palestra para os senhores, não só em razão do convite do Instituto dos Magistrados, mas também porque tenho um compromisso, no período da tarde, de falar sobre as questões civis. Então, essa primeira apresentação tem de ser espetacular para que todos possam voltar depois do almoço – período mais cansativo e pesado. Tenho certeza absoluta de que o auditório estará ainda mais cheio. Pior do que fazer uma apresentação após o almoço talvez seja dar aula aos sábados à tarde, mas, como faço isso há mais ou menos quatro anos, estou bastante acostumado.

Como já mencionado pelo Dr. José Carlos, sou sócio do Opice Blum Advogados Associados, que tem na pessoa do Dr. Renato Opice Blum um dos divulgadores do Direito Eletrônico. Digo que não se tem mais como fugir do Direito Eletrônico como um todo. Hoje mesmo, antes de vir para este Seminário, soube que aconteceram dois ilícitos nos Estados Unidos: os *twitters* do Barack Obama e da Britney Spears foram clonados, ou seja, alguém acessou indevidamente a base de dados, explorando alguma vulnerabilidade de quem utiliza a senha dos *twitters* do Barack Obama e da Britney Spears, e conseguiu fazer essa clonagem.

Recentemente, todos puderam acompanhar a questão da *cyberwar*, ou seja, os conflitos em relação ao *Google* na China, a questão da censura, uma questão constitucional para nós, brasileiros, sobre a liberdade de expressão; na China o *Google* saiu justamente em razão da imposição do governo chinês em relação à censura, ou seja, só pode ser divulgado o que antes for analisado; o *Google* acabou saindo da China, colocou o provedor em Hong Kong, mas, mesmo assim, está encontrando algumas dificuldades. E, depois que estavam tendo essas discussões, o *Google* sofreu um ataque DDoS, ou seja, *Distributed Denial of Service*, ataque em massa, em que normalmente são utilizados computadores

zumbis do mundo inteiro, computadores que são invadidos – nossos computadores podem estar sendo utilizados nesse momento – para simplesmente tirar do ar um provedor como o *Google*.

A grande origem desses ataques em massa foi identificada como sendo feita pelo próprio governo chinês, ou seja, este fato poderia criar uma instabilidade e, até mesmo, uma guerra virtual, uma *cyberwar*, como já aconteceu em alguns países relacionados ao assunto.

Outro ponto bastante interessante: recentemente dois representantes legais, também da empresa *Google*, na Itália, foram condenados criminalmente porque disponibilizaram no *You Tube* um vídeo de uma criança, com Síndrome de *Down*, sendo ofendida e espancada. Houve uma decisão judicial determinando a remoção do vídeo. É possível remover-se algo da internet? Por bem ou por mal, por mais que a empresa tentasse cumprir a ordem, não foi possível cumpri-la, porque sempre disponibilizavam novamente o vídeo. Em resumo, as pessoas físicas representantes da pessoa jurídica, no caso o *Google*, foram condenadas por esse ato.

Para os senhores terem uma ideia, no Brasil já são mais de 17 mil decisões judiciais sobre o tema Direito Eletrônico. Isto é a mais pura realidade. Começaremos a palestra *Questões Constitucionais em Direito Eletrônico* abordando justamente o Princípio da Legalidade ou da Reserva Legal. Será que no Brasil precisamos de uma legislação específica sobre esse assunto para cumprir o Princípio da Legalidade ou da Reserva Legal, principalmente para efeitos penais, em que não existe analogia, ou seja, em que o fato tem que ser definido como crime para haver o crime? Como temos 17 mil decisões judiciais se não há lei específica sobre o assunto?

No Brasil, temos a denominada *civil law,* ou seja, o direito positivado, temos leis para tudo; já nos Estados Unidos e em outros países prevalece a *common law*, ou seja, poucas legislações em que possa ser aplicado. Temos, por bem ou por mal, uma inversão desse conceito no Brasil sobre isso, porque, apesar de não termos muitas leis específicas

sobre o assunto, temos diversas leis esparsas que são plenamente aplicáveis. Obviamente, precisamos de alguns ajustes, mas lei existe.

Falando do aspecto criminal, podemos considerar que para 95% de todos os atos jurídicos que acontecem em favor das novas tecnologias ou contra elas já há um crime previsto. Teríamos uma defasagem de 5% para tipificação penal de condutas que hoje não existem.

Precisamos de uma melhora em outros casos, principalmente, relacionados à preservação de provas eletrônicas. Também, há crimes que têm penas pequenas e que, com o avanço da internet, o que antes não tinha uma ofensividade muito grande contra as vítimas, atualmente tem, porque o potencial lesivo da internet é enorme. Inclusive, traz novos tipos de conceitos.

Muitas vezes, o Poder Judiciário absolve uma pessoa – o que foi até comentado pelo Dr. José Carlos –, porém, a internet continua condenando-a. Como exemplo, podemos lembrar aquela festa de calouros ocorrida numa universidade de medicina em São Paulo, onde um dos calouros morreu afogado. Houve o processo judicial contra alguns veteranos e, na época desse procedimento judicial, saíram diversas informações em todos os tipos de mídia, inclusive obviamente na mídia eletrônica, principalmente sobre um dos veteranos que estava sendo acusado. Passados alguns anos, esse veterano foi absolvido pelo Supremo Tribunal Federal. A Justiça o absolveu, considerando que ele não havia cometido o crime, mas, até hoje, se formos pesquisar o nome da pessoa na internet, o que aparece? E quando qualquer um procura um médico, o que se faz? Verifica-se quem é essa pessoa. Ou seja, a Justiça absolveu, mas a internet continua condenando.

Devemos refletir bastante sobre essas questões atualmente para ponderar princípios constitucionais como a liberdade de expressão, mas a vedação do anonimato; a questão da privacidade, da intimidade, mas também o direito à propriedade das pessoas. Hoje em dia, não existe mais privacidade. Os magistrados precisam estar condizentes e coerentes

com essas novas tecnologias para julgarem uma causa de acordo com o potencial ofensivo que essas novas tecnologias trazem.

A Constituição Federal, art. 5º, afirma:

II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;

XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Exemplo prático. Sou um amigo seu. Esse é um aviso. Você está sendo traído. Não tive coragem de te falar, mas, como imagens falam mais do que palavras, faça o *download* das fotos e veja com os seus próprios olhos. Foi a única maneira que encontrei para te avisar.

Os senhores sabem que estou falando da prática de *fishing scan*, pescaria para fraude. Alguém manda milhares de mensagens como essa para que algumas pessoas acreditem, tenham os seus computadores desprotegidos e instalem o chamado Cavalo de Tróia. Por que Cavalo de Tróia? Porque se pensa estar recebendo um presente, mas, na realidade, a pessoa está instalando um código malicioso que, possivelmente, conseguirá monitorar e obter todas as informações do seu computador.

Antes de começarmos a debater as questões constitucionais,

dentro do Princípio da Legalidade, pergunto aos senhores se há algum crime somente com o envio dessa mensagem? Enviar código malicioso é crime no Brasil? O envio desse tipo de mensagem no Brasil não é crime. Não há nenhum tipo penal que preveja essa conduta como sendo criminosa. Os senhores acham que o envio de código malicioso deveria ser crime? Seria um crime de mera conduta? Por que não importa o resultado? Só o fato de enviar código malicioso seria crime? Será que devem existir crimes de mera conduta no nosso ordenamento jurídico? Por que existem os crimes de mera conduta? Porque são crimes preventivos, como o porte ilegal de arma. Não importa se o indivíduo dará ou não um tiro numa pessoa; basta estar portando ilegalmente uma arma que se configura um crime de mera conduta.

Podemos citar, também, a alteração recente que houve no Código de Trânsito brasileiro sobre dirigir embriagado. Não importa se a pessoa fala, em conversa de bar, que dirige melhor embriagado. Imaginem a seguinte situação: é feita uma perícia com uma pessoa embriagada e com uma sóbria, ambas dirigindo, e fique comprovado que a pessoa dirige melhor embriagada. Isso importa para o Direito Penal? Não. Basta estar dirigindo embriagado para ser considerado crime. Por quê? Por que deve-se esperar alguma coisa acontecer desse tipo de conduta? Não. Porque são condutas que têm um potencial lesivo muito grande. O Direito Penal se antecede e caracteriza como crime aquela simples conduta.

Atentem para a palavra maliciosos. Por que código malicioso e não vírus? Porque vírus, normalmente, só se propaga. Pode ser que não se tenha um vírus com um código malicioso. Pode ser que seja só com o intuito de se propagar. Mas quando se fala em código malicioso, é para fazer o mal. Nesse caso, quem dissemina milhares de códigos maliciosos deveria ser, na minha opinião, punido com o crime de mera conduta. Mas no Brasil ainda não há esse tipo penal.

Também não há, no Brasil, a invasão de domicílio virtual. Não é crime, no Brasil, alguém acessar a base de dados de uma empresa,

bisbilhotar os seus arquivos e não fazer nada com aquela informação. Por quê? Porque não há definição penal específica.

Se verificarmos no *firewall* das nossas empresas, dos nossos escritórios, dos nossos gabinetes – *firewall* é aquele programa que identifica o que está entrando e o que está saindo e bloqueia –, quantas tentativas de acesso indevido acontecem diária ou mensalmente? Milhares. Não é a mesma coisa de alguém que tenta pular o muro da nossa casa e recebe uma descarga elétrica? Só que no Brasil, isso não é crime; portanto, enviar código malicioso não seria crime.

Os senhores poderiam questionar que eu comecei falando que no Brasil 95% dos atos já têm previsão e agora faço uma introdução mencionando dois atos que não têm nenhuma definição legal.

Vamos continuar com esse estudo.

O sujeito enviou esse tipo de *e-mail*. A pessoa, a vítima, acreditou. Não tinha um antivírus atualizado e baixou o código malicioso. O quê esse código malicioso vai fazer? A partir do momento em que ele acessar o *internet banking* nele, as informações que iriam para a instituição financeira irão para o fraudador. E agora, temos um crime nesse tipo de situação? Sim ou não? O quê os senhores acham?

Se alguém colocar uma ferramenta no telefone celular dos senhores e começar a interceptar a comunicação telefônica, isso não é crime? Sim. Onde está a previsão sobre isso? Na Constituição, art. 5º, inciso XII, que fala da inviolabilidade das comunicações, e na Lei nº 9.296/96 que regulamenta os referidos artigo e inciso. E o que essa Lei preceitua? Que são invioláveis as comunicações telefônicas, as comunicações telemáticas e as comunicações informáticas. E, no art. 10, tem o crime previsto para quem, sem uma ordem judicial, durante a instrução processual penal, pratica a interceptação de comunicações telefônicas, informáticas ou telemáticas. E até que a pena é bem razoável: reclusão de um a quatro anos.

Então, a partir do momento em que a informação não está indo mais para o banco, mas para o fraudador, seria uma interceptação de comunicações telemáticas ou informáticas. Já temos um crime. Está começando a ficar melhor.

Vamos prosseguir. O que o sujeito faz depois? Pega os dados da vítima na instituição financeira e acessa a conta bancária da mesma. Coitado do fraudador. A vítima não tinha onde cair morta. Quase que o banco foi atrás do fraudador para pegar empréstimo em razão do que a vítima devia. Não fez a fraude porque não tinha patrimônio na conta. Temos ou não um crime com essa conduta? Qual o crime? Nesse caso, para que ele soubesse se a vítima tinha ou não tinha patrimônio, o que ele acessou? O extrato bancário. Quebra de sigilo bancário, crime previsto na Lei Complementar nº 105/2001.

Outra questão interessante: a partir do momento em que o fraudador acessou o *internet banking,* para o banco o acesso teria partido do cliente, então vítima. Tem-se ou não outro crime? Tem um mais específico, que é a falsidade ideológica mais o crime de falsa identidade, art. 307 do Código Penal: aquele que pratica, usa a identidade de terceiro para obter vantagem ou causar prejuízo. Falsa identidade.

Interceptação de dados telemáticos ou informáticos, falsa identidade, quebra de sigilo bancário.

Por sorte do fraudador e infelicidade da vítima, ela tinha patrimônio no banco. O criminoso fez a transferência bancária. E agora? Temos um crime ou não? Apropriação indébita? Estelionato? Furto mediante fraude? Estelionato ou furto mediante fraude? Difícil, não é?

Estelionato é o crime mais charmoso do Código Penal. Muitos falam que nem deveria ser crime, porque o criminoso leva a vítima a tal engano que a própria vítima entrega o bem para o estelionatário. Derivado do latim *stellio*, nome de uma espécie de lagarto que muda de cor para passar despercebido. É o famoso art. 171 do Código Penal. Quando dou

aula para turmas de segurança da informação, que não têm conhecimento jurídico, sempre começo falando que eles têm conhecimento jurídico. Quando pergunto qual é o artigo do estelionato, todos respondem 171. Estelionato. A vítima entrega o bem ao fraudador.

E o furto mediante fraude? Forma qualificada do furto? A fraude é empregada para tirar a vigilância do bem da vítima para, depois, subtraí-lo. Subtrair, para si ou para outrem, coisa alheia móvel (art. 155 do Código Penal) – só estou fazendo uma introdução das questões constitucionais, porque o Dr. Augusto Rossini dará um show amanhã. O que é coisa? Um *notebook* é uma coisa? Uma carteira é uma coisa? Uma caneta é uma coisa? É algo palpável, tangível, certo? O que foi subtraído? Foi dinheiro – papel – ou patrimônio? Quase não temos mais dinheiro. Daqui a pouco não existirá mais. Foi feita uma transferência eletrônica. Isso é palpável, é tangível? Imaginem se num processo o advogado de defesa alegar que aquela conduta é atípica porque o promotor de justiça denunciou o seu cliente por furto mediante fraude e o que foi subtraído não é palpável, não é tangível, mas meras informações eletrônicas. O promotor de justiça, provavelmente, utilizará um laudo do Instituto de Criminalística ou um assistente de acusação para explicar do que é feita uma informação eletrônica.

Tecnicamente, do que é feita uma informação eletrônica? Do que é feito esse *slide* que está aqui no computador? *Bits e bytes.* O que é um *bit*? Uma combinação binária de zeros e uns. O que, normalmente, faz o zero deixar de ser zero para passar a ser um? Um impulso elétrico. Olha, se alguém quiser saber se isso que aconteceu é algo palpável, tangível, para fins jurídicos, é só colocar o dedo na tomada e observar se vai levar um choque. Imagine chegar a esse tipo de situação. Estou dando esse exemplo, porque, muitas vezes, os laudos técnicos têm que chegar até esse tipo de profundidade para demonstrar que não se está falando de analogia, mas de realidade.

E mais, o princípio de coisa é valor ativo dentro do Direito.

Portanto, já existem decisões, inclusive em superior instância, falando que não importa se a coisa é palpável ou tangível e, nesse sentido, poderia ser caracterizado o furto mediante fraude. Mas a dúvida é latente, se é furto mediante fraude ou estelionato. A maioria das decisões judiciais vai pelo caminho do estelionato. Não tem a discussão da coisa e, por bem ou por mal, por que o estelionato? Porque uma das vítimas desses casos são os bancos.

Na segunda parte, discutiremos a responsabilidade civil *internet banking*. O banco está sendo enganado, pensando que está entregando o bem para o seu cliente, mas o está entregando para o fraudador, que seria o estelionato. Sou um pouco mais favorável a essa corrente.

Temos interceptação de dados telemáticos ou informáticos, falsa identidade, quebra de sigilo bancário, furto mediante fraude ou estelionato, mais tendente para o estelionato. Coitado do criminoso ou será que temos mais alguma conduta? Esses criminosos têm que pensar, principalmente, na mente masculina do aspecto da traição, para elaborar um *e-mail* como esse. Nesses *e-mails* é preciso chamar a atenção; sempre tem um texto dentro de um contexto. Acontece algum acidente, vejam aqui as fotos do acidente tiradas na sequência; vejam as fotos que tiramos no verão passado. Esses *e-mails* são enviados por pessoas conhecidas, porque os computadores delas estão infectados.

Uma vez, no meu serviço de mensagem instantânea, apareceu uma caixinha com a seguinte mensagem: Rony, você viu as fotos que tiraram de você? Como não faço nada de errado, não fiquei preocupado, mas assusta um pouco. Tratava-se de uma montagem de fotos. Por eu ser um profissional da área, liguei para saber o que estava acontecendo, e o computador dele havia sido infectado. Por isso, temos que desconfiar de tudo e, acima de tudo, termos os nossos computadores protegidos com antivírus atualizado, *firewall*, programas de computadores e *softwares* sempre lícitos e atualizados. Enfim, o criminoso precisa criar esse *e-mail*, ter essa ideia.

De que mais ele precisa? Ter milhares de contas de *e-mails* para que sejam destinatárias dessa mensagem. Ele precisa fazer o código malicioso, inseri-lo na mensagem e enviá-la. Ao enviar a mensagem, o criminoso fica esperando para ver quem cairá na pescaria, no *fishing.* Diante das informações, ele escolhe as que lhe interessam. A mesma pessoa acessa a conta do banco, faz as transferências, saca dinheiro direto no caixa. É o super-homem do mal que faz isso? É uma só pessoa que faz tudo isso? Normalmente, não. Mais de três pessoas para a mesma finalidade criminosa. Art. 288 do Código Penal: formação de quadrilha.

Então, temos uma série de crimes. No Brasil, sobre esses assuntos ou mais especificamente sobre fraude *internet banking* já existem pelo menos 30 decisões judiciais e algumas já condenando esses criminosos a mais de 17 anos de reclusão, porque, no caso, entra a questão de o crime ser de forma continuada, se há concurso material ou formal, mas, justamente em razão dessa pescaria que é feita, muitas vezes, de uma vítima ele só intercepta, de outra, quebra o sigilo bancário e só de uma outra terceira vítima é que ocorre a fraude, ou seja, o crime fim, pelo Princípio da Consunção, não seria absorvido pelos outros crimes porque as vítimas foram diferentes. Por isso, as penas são tão altas.

Trouxe esse primeiro exemplo para mostrar um pouco desses 95% que temos de legislação aplicável sobre o assunto. A expectativa da Polícia Federal é que, daqui a 5 ou 10 anos, 90% de todos os ilícitos tenham algum tipo de nova tecnologia empregada.

Ainda dentro do Princípio da Legalidade, o que precisamos adequar dentro dessa questão? Acredito que todos aqui ouviram falar do projeto de lei, que é um substitutivo a três projetos de lei, de autoria do Senador Eduardo Azeredo. Depois, deixou de ser um projeto do Senador Eduardo Azeredo, passando a ser um projeto do Senado Federal. Esse projeto de lei, que foi chamado por alguns de AI-5 digital – na minha opinião, de forma completamente equivocada; obviamente nenhum projeto é perfeito, assim como nenhuma lei é perfeita –, trazia principalmente essas novas tipificações penais como, no caso, o acesso não autorizado à rede de computadores, a divulgação indevida de informações, danos por difusão de código malicioso, a própria difusão de código malicioso, falsificação de cartões de crédito e débito e, principalmente, a responsabilidade civil – e não penal – daquele que provê acesso à internet.

Outra questão constitucional que muitas vezes as pessoas se esquecem, principalmente quem pratica atos ilícitos na internet, é que no art. 5º, inciso IV, da Constituição Federal, onde está prevista a liberdade de expressão, está vedado o anonimato, ou seja, por esse simples princípio constitucional seria possível quebrar o sigilo e identificar uma

pessoa.

Normalmente, para quase todos os atos ilícitos praticados através dos meios eletrônicos, ou as pessoas utilizam a identidade de terceiros ou estão no anonimato. Identificam-se os fraudadores através dos provedores de acesso à internet, porque todos recebem um protocolo de internet e têm um contrato de acesso, ou seja, quando alguém pratica o ilícito – isso é o interessante no Direito Eletrônico, por mais que seja difícil, sempre há um vestígio – é possível se identificar. Se o provedor de acesso à internet não tiver a informação de qual usuário tinha aquele IP – I*nternet Protocol*, naquela data e naquele horário, normalmente inviabiliza uma investigação.

Comentamos sobre a questão do *Google* na China. No Brasil, há três ou quatro anos, o Ministério Público Federal travou uma batalha gigantesca contra essa mesma empresa, em razão da falta de registros eletrônicos de crimes vinculados à pornografia infantil e ao tráfico de entorpecentes. Na época, foi proposta uma ação civil pública, com vários requerimentos de multa e, inclusive em última instância, de fechamento da empresa aqui no Brasil. Felizmente, chegou-se a um consenso e cada vez mais se forma o termo de ajustamento de conduta, justamente para que esses registros eletrônicos sejam preservados de uma forma coerente.

Sobre a responsabilidade dos provedores, deixarei para a palestra depois do almoço, porque assim poderemos tratar um pouco mais sobre a responsabilidade civil. Talvez a questão mais importante desse projeto seja a guarda de registros eletrônicos, porque, sem isso, normalmente não é possível se fazer qualquer investigação. Para os senhores terem uma ideia do andamento desse projeto de lei, ele foi para a Câmara dos Deputados e, provavelmente, não será aprovado. Deve-se fazer um novo projeto de um marco regulatório civil, quer dizer, fazer uma legislação civil antes de uma legislação penal sobre o assunto. Se for feita de forma coerente, ótimo, os advogados terão mais ferramentas para trabalhar.

Comentando alguns pontos importantes da questão legislativa, desse Princípio da Legalidade, para se ter uma ideia, em questões bem técnicas jurídicas, a interceptação lícita, ou seja, com ordem judicial, dentro de uma investigação penal, só pode ser deferida se o crime que estiver sendo investigado for de reclusão. O problema é que normalmente uma investigação eletrônica depende dessa interceptação lícita, preciso saber o que está trafegando no computador do bandido.

Ocorre que, para diversos atos ilícitos, como por exemplo, crime contra a honra, ameaça, concorrência desleal, crimes empresariais, em que o indivíduo aperta um botão e transfere toda a informação confidencial para o concorrente, a pena é de detenção, ou seja, não dá para se ter uma ordem judicial de interceptação de dados. Isso porque, ressaltando que o avanço da tecnologia traz esse potencial lesivo, deveria haver uma modificação na nossa legislação para possibilitar a interceptação de dados telemáticos ou informáticos, mesmo para crimes punidos com detenção, se praticados por meios eletrônicos. Pode-se dizer que seria uma devassa das pessoas, mas precisa-se de ordem judicial, ou seja, tem um magistrado analisando se é o caso de interceptação ou não.

Da mesma forma a prisão preventiva, em que um dos requisitos é a questão da pena, a reclusão, e hoje em dia o criminoso pode acabar com a vida de uma pessoa, como em alguns casos que vou contar aqui, através da internet, praticando crimes contra a honra, trazendo um perigo iminente, até muitas vezes de ordem pública, e não pode haver uma prisão preventiva.

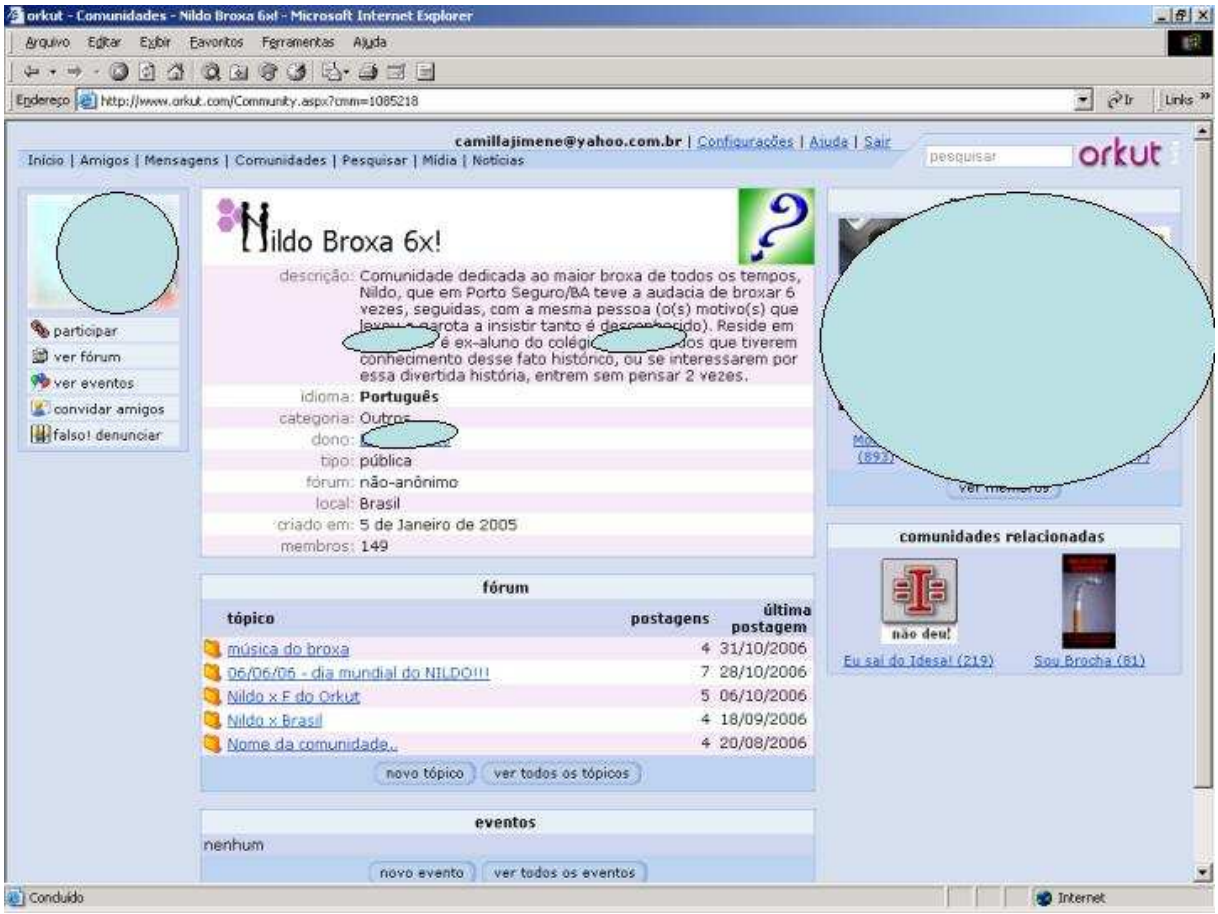
No caso de crimes contra a honra, a pena é muito baixa, não ultrapassa dois anos. Comentaremos isso daqui a pouco.

Definição de provedores. Como estava no projeto de lei, a definição de provedores, aqueles que são obrigados a guardar esses dados, estava descrito como aqueles que provêem acesso à grande rede mundial de computadores comercialmente ou a entidades públicas. O problema é o "comercialmente". Quem estaria dentro? Somente as Operadoras de

Telecom que realmente provêem acesso ou uma pizzaria que tem um W*i-Fi* que dá acesso aos seus clientes? Dessa forma, ficaria muito simples. Quem quisesse praticar algum ilícito iria a uma pizzaria, que não tem nenhum controle de identificação, enviaria um *e-mail* ou acessaria a base de dados, passando a informação para o concorrente, na certeza de que não seria identificado. Ou seja, esse tipo de responsabilidade precisa abranger a todos. Precisamos definir bem o que queremos no Brasil: uma internet livre, como tem que ser, e é impossível não ser, mas com segurança, ou um "faroeste", onde ninguém é identificado e nem obrigado a nada. Então, como portas de entrada e saída da rede, os provedores permitem, quando se tem um ato ilícito, que se faça uma investigação e, conseqüentemente, haja uma punição dentro do devido processo penal.

Outro ponto importante do projeto de lei. Existe a Convenção de *Cibercrime*, que é a Convenção de Budapeste, que já conta com mais de 42 países signatários. Segundo essa Convenção, quando existir um ato ilícito, deve haver a troca rápida de informações entre países signatários para identificar e punir. O Brasil poderia hoje ser signatário dessa Convenção? Até poderia, mas com diversas restrições, porque se o Brasil não tem uma lei específica sobre preservação de dados eletrônicos, não teria como ser signatário sem algumas restrições, não poderia contribuir. Mais uma vez, a importância da aprovação de uma lei especifica com esses pequenos detalhes, que provavelmente será esse marco regulatório civil.

Passemos aos princípios fundamentais previstos na Constituição Federal. Dignidade da pessoa humana.



Nildo broxa 6X. Comunidade dedicada ao maior broxa de todos os tempos, Nildo – desculpem-me pelos termos utilizados, mas é um exemplo prático –, que, em Porto Seguro/BA, teve a audácia de acontecer isso seis vezes seguidas com a mesma pessoa. Contém foto, nome, cidade e local onde o indivíduo trabalha. Onde está a dignidade da pessoa humana? Essa notícia foi, obviamente, espalhada ao mundo, porque, uma vez que foi parar na internet, qualquer um pode acessar.

Conto um caso bem prático que mostra justamente como, muitas vezes, pode deixar de existir essa dignidade da pessoa humana em se tratando de Direito Eletrônico. Um homem casado, de mais ou menos quarenta anos de idade, trouxe-nos um *notebook*, mostrando um *e-mail*, dizendo que a vida dele estava acabando. Na leitura desse *e-mail*, percebia-se que o autor, teoricamente, seria uma mulher, que, anonimamente, contava a vida inteira dele, falando que sabia onde ele

trabalhava, sabia que ele era casado, sabia que ele tinha uma filha de três meses, sabia que ele tinha relacionamentos extraconjugais, que tinha fotos e vídeos desses relacionamentos e que, a partir daquele momento, a vida dele, tanto pessoal quanto profissional, iria acabar, porque começaria a divulgar isso para todos. Que situação! O quê fazer agora? Questionamos se o conteúdo do *e-mail* era verdadeiro, e o homem nos informou que a maioria das informações ditas na mensagem era verdadeira e que, acerca de relacionamento extraconjugal, apenas brincava na internet com algumas pessoas, mas nunca tinha feito nada além daquilo.

Como identificar essa pessoa? Nesse caso, está caracterizado o crime de ameaça, porque foi dito no *e-mail* que a vida daquele homem iria acabar. A solução seria verificar o IP – o protocolo de internet do *e-mail*. Esse IP tinha origem na Ucrânia. Será que foi um ucraniano que cometeu esse ilícito? Não. Assim como existem os paraísos fiscais, existem os paraísos virtuais, os *proxys* abertos, ou seja, provedores de acesso aberto para mascarar o verdadeiro IP. Então, não era possível identificar.

Nesse caso, a solução seria ingressar com uma ação contra o único contato que tínhamos com esse ou essa criminosa (o), qual seja, a conta de *e-mail* utilizada, porque, para enviar a mensagem, utilizou-se uma conta de *e-mail*. Por que fomos atrás dessa conta de *e-mail*? Será que a pessoa apresentou CIC, RG, CPF e comprovante de residência para abrir uma conta de *e-mail*? Os senhores apresentam esses documentos para abrir uma conta de *e-mail*? Será que deveríamos apresentá-los? Com certeza, seria muita burocracia. Mas, vejam que interessante: para abrir uma conta no banco e para diversos outros atos jurídicos não precisaríamos fazer isso? Aliás, a validade jurídica da palestra anterior, para algum advogado ou o Poder Judiciário atuar dentro do processo eletrônico, está dentro da Medida Provisória nº 2.200/01, que trouxe a Infraestrutura de Chaves Públicas Brasileiras. Segundo essa Medida Provisória, para termos um certificado digital, precisamos nos identificar e

apresentar os documentos, pedir para sermos nós mesmos através da internet, para recebermos o certificado digital. Enfim, não vamos entrar nessa discussão.

Se não obteríamos essas informações naquela conta de *e-mail*, por que pedir uma ordem judicial de quebra de sigilo daquela conta? Para sabermos todos os registros eletrônicos utilizados no acesso àquela conta, porque, às vezes, pode-se utilizar um IP ucraniano para enviar o *e-mail*, mas não o utilizar para simplesmente acessar. E se ele acessou da casa dele, da universidade onde estuda? E se ele acessou do trabalho outra vez? Ou seja, ali existe um rastro dos acessos.

Entramos com a ordem judicial. Ordem judicial deferida. Presentes os requisitos. Uma coisa é termos essa expectativa.

No dia seguinte, depois do envio dessa mensagem, mensagem enviada para a esposa do sujeito, contendo fotos e vídeos dele com outras pessoas; no outro dia, mensagens enviadas para todos os contatos pessoais dele e da esposa, com as mesmas fotos e vídeos nas situações mais constrangedoras que os senhores possam imaginar; no outro dia, *e-mail* enviado para todos os contatos profissionais dele. Estavam acabando com a vida pessoal, profissional e com a dignidade dele. Se ele fosse proferir uma palestra pela empresa, com uma simples pesquisa no *Google*, descobria-se não só onde seria a palestra, mas todas as fotos e vídeos enviados para os contatos da organização.

Finalmente, veio a resposta do provedor de conta de *e-mail* com todos os registros eletrônicos: Ucrânia, Canadá, Estados Unidos, tudo mascarando o IP, e havia um IP do Brasil. Pedimos, então, uma ordem judicial para quebrar o sigilo desse IP do Brasil. Presentes o **fumus boni juris** e o perigo de demora, ordem judicial deferida. Enquanto isso, havíamos instaurado o inquérito policial, porque não dava mais para aguentar a situação. Veio a informação do provedor e nela havia um registro de uma residência, no interior de São Paulo. Existe uma ordem judicial, já se sabe do local, o que fazer?

Vamos para outro princípio constitucional, art. 5º, inciso XI:

> A casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial.

Os senhores acham que seria o caso de flagrante? O crime está pegando fogo? Não, já aconteceu. Poderíamos ter sorte, mas não estava em estado de flagrância. Caso de desastre ou para prestar socorro? Não parece ser o caso. Ou, então, mediante ordem judicial, durante o dia.

Tínhamos o inquérito. Levamos ao delegado as informações e pedimos que representasse ao juiz competente uma busca e apreensão. O delegado, por sua vez, não considerou aquilo como um crime; disse que era coisa de marido e mulher e que não faria a representação porque provavelmente o juiz não iria deferir pela busca e apreensão.

A cada dia que passava, novas mensagens eram envidas, e a vítima chegou a ponto de dizer: "Não quero mais saber de justiça criminal ou justiça cível. Só quero que isso pare".

Estamos diante de um criminoso cibernético. Quando que, normalmente, algum criminoso pára de praticar o ilícito contra a dignidade da pessoa humana como esse? Quando? Acima de tudo, eles são covardes, porque os tímidos também podem praticar crimes, já que estão atrás do computador, agindo anonimamente; não sabem, muitas vezes, nem quem é a vítima. Por isso, são covardes. A nossa conclusão foi informar ao criminoso que já havíamos identificado a autoria.

Como fazer? Mandar um *e-mail* de volta para a pessoa, informando que ela já havia sido identificada? Enviar uma notificação? Não. Melhor ainda, entramos com uma ação inibitória, uma obrigação de não fazer, requerendo uma multa, para que – tínhamos o local do ilícito, mas não a autoria – aquela pessoa que saiu como responsável pelo contrato de acesso à internet se abstivesse daquela prática ou tomasse as medidas necessárias para que, do seu contrato de acesso à internet, essa prática não fosse feita novamente.

Com a ação inibitória, obrigação de não fazer, a prova do provedor, a fumaça do bom direito, os *e-mails*, mais a informação do provedor, **periculum in mora** é o mesmo, o juiz entendeu que não era o caso, ainda, de deferir a liminar. Ele designou uma audiência de justificação para conversar com o autor e o réu e decidir se concederia ou não a liminar. Essa audiência foi marcada para a semana seguinte.

Mesmo sem a liminar, fomos para a audiência. Na sala de audiência, entram o advogado da parte contrária e um senhor de mais ou menos 65 anos de idade. Pensei: meu Deus, o que está acontecendo aqui? E agora? Perguntei para a vítima se ele conhecia aquele senhor; ele disse que não tinha ideia de quem era.

O juiz perguntou para o réu se ele tinha conhecimento dos autos e do que estava acontecendo – enquanto isso, estávamos esperando a busca e apreensão no Tribunal Criminal. Os senhores poderiam me perguntar se isso não poderia estragar a prova? Poderia. Mas, por bem ou por mal, eles não sabiam que estávamos aguardando uma busca e apreensão. O réu disse que não tinha nada a ver com aquilo, que era um absurdo e que iria processar a todos por fazê-lo passar por aquela situação.

Perguntas do ilustre advogado. O que os senhores perguntariam?

– O senhor tem acesso à internet em sua casa?

– Sim, tenho.

– Utiliza a linha discada ou banda larga?

– Banda larga.

– Qual o provedor que o senhor utiliza?

– Utilizo o provedor X.

Era o mesmo.

– Há quanto tempo o senhor utiliza esse provedor?

– A X período de tempo.

Todas as respostas bateram. E agora. O quê mais poderíamos perguntar? Sabíamos que tinha partido da casa dele.

– Quem mais acessa a internet na sua casa?

– Eu, minha mulher e meu filho.

– Só os três?

– Sim.

O que os senhores perguntariam agora?

– Seu filho tem quantos anos? E sua mulher?

– Minha mulher tem mais ou menos a mesma idade que a minha, e meu filho tem 26 anos de idade.

Isso tudo para conseguir a liminar.

E agora? O sujeito mascarava os IPs, utilizada *proxy* da Ucrânia. Deve ter certo conhecimento.

– O que seu filho faz da vida? O que ele estudou?

– Meu filho não faz nada há muito tempo, mas ele é perito em Tecnologia da Informação pela Nasa.

Não falou Nasa, mas praticamente falou isso. Fantástico! Partiu de lá. O filho tem 26 anos, não tem muito o quê fazer da vida, ou seja, tempo de sobra, e um conhecimento absurdo em TI. O juiz indagou se havia mais alguma pergunta e eu disse que não. Quase que eu falei: pode conceder a liminar. O juiz não ficou convencido e nomeou uma perita judicial para realizar uma perícia nos computadores do réu no prazo de 10 dias.

O que os senhores acham disso? Seria muito fácil trocar todos os computadores da casa, e, dentro do prazo estipulado de dez dias, a perita não encontraria mais nada.

– Excelência, pela ordem. Em razão da nova decisão judicial de V. Exa., requeiro a imediata busca e apreensão dos computadores na casa

do réu, uma vez que, um simples contato de quem está aqui assistindo a esta audiência, com o mundo externo, pode dar uma ordem para apagar todas as provas. Portanto, além da busca e apreensão, todos aqui têm que ser mantidos dentro da sala de audiência, sem comunicação externa, a não ser com a perita, porque há um grande risco de perda de provas.

– Indefiro o seu pedido.

Desabafei para não ser preso por desacato à autoridade até os limites possíveis. Falei o que estava acontecendo. Expliquei um pouco sobre Direito Eletrônico, o que aquelas provas significavam, que o meu cliente estava com uma sensação de injustiça tremenda, além do que ele já estava passando, por uma nova decisão como essa. Expliquei novamente que todas as provas seriam perdidas, que seriam apagadas, que não conseguiríamos mais comprovar a autoria daqueles ilícitos. E saí da audiência.

Descemos do Fórum e ao lado havia um restaurante. Fomos até lá para nos acalmar. Depois de cinco ou dez minutos, tocou meu celular.

– É o Dr. Rony que está falando?

– Sim, pois não.

– Um minutinho só que o Juiz vai conversar com o senhor.

Pensei que ele fosse mandar me prender.

– Dr. Rony?

– Pois não, excelência.

– Fiquei meio preocupado com o que aconteceu na audiência e resolvi ligar para a perita judicial que eu havia nomeado para saber se realmente existia esse perigo de perda de provas e, realmente, ela me disse que sim e que a prova pericial iria ser realizada imediatamente.

– Que bom, Excelência.

– O Senhor pode ir lá com a perita agora, para que seja feita a clonagem dos computadores do réu?

– Sim, Excelência, estou aqui ao lado do Fórum.

– Ótimo.

Oficial de justiça, perita, tudo certinho, conseguiram preservar as provas; os computadores foram clonados.

Resumindo a história, durante mais de três anos, o filho daquele senhor se passava por uma mulher, através da internet, e tinha um relacionamento virtual com a vítima. Durante esses três anos, obviamente, a engenharia social permitiu que obtivesse todos os tipos de arquivos que quisesse, todos os tipos de prova, infectou o computador da vítima – foi assim que ele conseguiu a senha de acesso às contas de *e-mail* para obter todas as contas de *e-mail* que foram utilizadas para a disseminação das fotos e vídeos.

Vejam que interessante. Por isso, trouxe esse caso em relação à dignidade da pessoa humana.

Parte da denúncia do Ministério Público. O sujeito foi denunciado pelo crime de interceptação de dados telemáticos ou informáticos e pelo crime de ameaça diversas vezes.

> Consta também que no interstício de tempo compreendido entre os dias 15 de junho e 31 de setembro de 2004, o Denunciado, abusando de seus conhecimentos informáticos, realizou interceptação de comunicação informática ou telemática, violando e alterando a senha secreta da vítima, acessando sua caixa postal eletrônica e lesando sua intimidade. Consta que o Denunciado, devido à citada interceptação, logrou conhecer todos os contatos pessoais da vítima, utilizando-os posteriormente em sua saga difamadora empreendida contra esta.
> Desta forma, o Denunciado, havendo realizado a interceptação informática ou telemática no correio virtual da vítima, fazia-se passar por esta perante terceiros, mantendo conversas íntimas com seus conhecidos, consoante se nota a fls. 92/119. Em outras oportunidades, o Denunciado, por meio dos contatos obtidos com a citada interceptação informática, enviava *e-mails* contendo pornografia e situações constrangedoras da vítima (fls. 489/492) para todos os seus conhecidos, o que servia para difamá-la perante seu círculo de relacionamento íntimo e profissional, dando causa a um verdadeiro tormento e desassossego em sua vida social.

Eu não seria tão criativo para inventar uma história como essa, mas é a pura realidade. Esse foi um dos casos mais complicados de que cuidamos.

Empresário acusado de filmar mulheres em banheiros é condenado a indenizar vítima.

Temos que ter muito cuidado com a questão da privacidade, da dignidade da pessoa humana.

Em São Paulo, adolescentes e jovens, no metrô, colocaram o celular no tênis para filmar em baixo das saias das mulheres e ainda tiravam foto para vincular a saia com a mulher, enfim, um verdadeiro absurdo. Por isso, temos que ter muito cuidado quando falamos em legislação, como dignidade da pessoa humana, porque são atos gravíssimos e que, atualmente, as penas são muito baixas para qualquer tipo de conduta como essa.

Art. 5º, inciso V: é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem. Outro direito e dever individual de qualquer cidadão.

Trago outro caso para os senhores.

Um ex-namorado pegou uma foto normal da ex-namorada, recortou o rosto dela, pesquisou um corpo de uma mulher nua na internet, compatível, e fez uma montagem no *fotoshop.* Criou um *e-mail* com o nome da ex-namorada, pegou todos os contatos pessoais e profissionais dela e enviou esse *e-mail*, anexando a foto montada, com os seguintes dizeres: "Pessoal, tive alguns problemas no meu trabalho. Agora, estou tendo que me prostituir para não morrer de fome. Seguem meus telefones celular e residencial para quem quiser fazer contato." O sujeito fez isso. É um absurdo.

Para esse tipo de conduta de difamação e injúria, a pena no Brasil não supera dois anos. Juizado Especial Criminal: cesta básica ou prestação de serviço à comunidade.

Mais uma necessidade de alteração da nossa lei, porque quando o legislador criou os crimes contra a honra, calúnia, injúria e difamação, ele não tinha como saber que a internet traria esse potencial lesivo. Um crime contra a honra pode ser algo "simples", compatível com a pena que existe atualmente, ou algo absurdo como esse caso que acaba com a vida de uma pessoa, e a pena é a mesma.

Deveríamos ter uma alteração na nossa legislação para permitir que o juiz possa aplicar uma pena maior, dependendo do tipo de conduta.

Ou seja, ter uma pena máxima maior para o crime contra a honra.

Explicamos a essa vítima que, se fosse pelo lado criminal, ela iria considerar, cada vez mais, o mundo injusto, que o Direito não tinha sentido. Por isso, a aconselhamos pleitear uma indenização civil. Juntamos todas as provas, depois de quebrar o sigilo da conta de *e-mail* – porque ele estava se passando por ela –, identificar que aquele *e-mail* partiu da casa do ex-namorado e fazer a busca e a apreensão comprovando tudo isso. Vejam a dificuldade para se descobrir um crime como esse.

O Juiz da Primeira Instância da Comarca de Teófilo Otoni, interior de Minas Gerais, concedeu R$ 5.000,00 (cinco mil reais) de indenização por danos morais. Um absurdo! Por mais que juntássemos todas as provas pertinentes, ele não saberia o potencial lesivo causado à vítima.

Recorremos ao Tribunal de Justiça – ainda bem que existe o duplo grau de jurisdição no Brasil. Reformada a decisão, foi concedido o valor de R$ 100.000,00 (cem mil reais) de indenização.

O sujeito não tem onde cair morto. Provavelmente, ela nunca receberá essa indenização, mas só o fato de ligar para a vítima e dizer que a decisão foi reformada e o valor da indenização aumentado para R$ 100.000,00 (cem mil reais), a sensação de justiça é muito grande.

Está aqui a decisão judicial do Tribunal de Justiça de Minas Gerais. Comprovada a situação vexatória e humilhante a que a vítima foi exposta, ficou demonstrada a gravidade e repercussão dos danos na vida da vítima. Por todo o exposto, dou provimento ao recurso de apelação para o fim de majorar o valor de indenização para R$ 100.000,00 (cem mil reais).

Caso recente que envolveu um piloto brasileiro em comunidades do *Orkut*, onde havia difamações – vou falar mais sobre isso em responsabilidade civil. Nesse caso, tudo vinculado ao art. 5º, inciso V, da Constituição, a imagem, a questão da dignidade. Neste caso, houve uma indenização de mais de R$ 500.000,00 (quinhentos mil reais) em Primeira Instância.

Mulher traída mostra namorado de *lingerie* na internet.

É o cuidado que devemos ter, porque não sabemos o que pode acontecer.

Mais um caso: privacidade e intimidade.

São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito de indenização pelo dano material ou moral decorrente de sua violação. Art. 5º, inciso X, da Constituição.

Casal de namorados em praias na Espanha.

É um caso de Direito Eletrônico puro, porque envolve bem essa questão de privacidade e intimidade. Os senhores se lembram do que aconteceu nesse processo? A pessoa pegou uma câmera e filmou por mais de uma hora aquele casal. Depois, fez uma montagem com as melhores cenas que reputou, inseriu uma música de fundo e disponibilizou na internet. Foi movida uma ação judicial para

tirar esse vídeo da internet.

Se os senhores fossem juízes, tirariam ou não esse vídeo da internet? Pergunta jurídica: qual a função desse vídeo permanecer na internet? Há algum direito à informação, relacionado a esse assunto, perto da imagem da pessoa, da dignidade da pessoa? Na minha opinião, por mais que, naquele momento, eles não tenham tomado as cautelas que deveriam ter tomado, não há qualquer motivo para aquele vídeo permanecer no ar; portanto, deveria ser removido.

Decisão da Justiça de Primeira Instância em São Paulo: estavam em um local público, são pessoas públicas, permanece o vídeo no ar.

Decisão em agravo de instrumento. Segunda Instância. Tribunal de Justiça do Estado de São Paulo: dois votos a um para tirar o vídeo do ar.

Como se tira um vídeo do ar? Por meio da URL, do nome do vídeo. Então, remove-se aquela URL, aquele nome do vídeo. Se houver a alteração de uma letra, qualquer modificação, o vídeo volta para o ar de novo. O que está acontecendo? O descumprimento de uma ordem judicial.

Os senhores se lembram do que aconteceu naquele episódio? O desembargador relator determinou que os provedores de *backbones* do Brasil não permitissem mais que IP's brasileiros, protocolos de internet do Brasil, pudessem acessar o *You Tube.* Dois *backbones* foram intimados e tiraram o *You Tube* do ar. Houve aquela comoção social e, de fato, deveria existir, porque o direito individual não pode prevalecer sobre o direito de todos. O juiz reconsiderou a sua decisão e determinou que o *You Tube* empregasse ferramentas para tirar aquele vídeo do ar.

Nesse caso, falo da privacidade, da intimidade. Na minha opinião, por mais que haja um deslize ali, não há porque manter aquilo na internet. O que possibilitou aquele vídeo permanecer na internet foi uma tecnologia em que a pessoa ficou filmando por mais de uma hora a cena acontecer. Depois, fez uma montagem, dando um tom mais pejorativo.

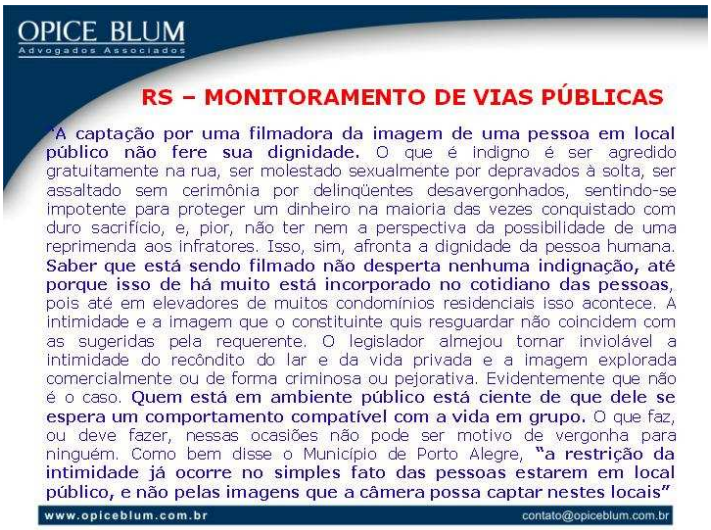
Imaginem se o casal não tivesse feito nada fora d'água. Se

tivessem esperado para se encontrar dentro d'água – só para os senhores terem uma ideia de exemplos – e chegasse um mergulhador para filmar dentro d'água. Pode existir? Pode. Temos que tomar cuidado, como em outros casos envolvendo esse tipo de situação.

Google maps. Serviço fantástico do *Google,* disponível em algumas capitais do Brasil. Além de ver o mapa das ruas por meio do GPS, vários carros dessa empresa têm um globo com câmeras para filmar todas as ruas em 360º, para que a pessoa possa não só ver o mapa, mas passear pelas ruas. Fantástico! O que acontece? Neste *slide,* não dá para ver direito, mas temos uma mulher saindo de um carro e, na hora em que foi sair, ela se debruçou um pouco e apareceu metade da calcinha justo na hora que estava passando o carrinho da empresa. Isso foi parar na internet. A pessoa está em um local público, mas, pelo amor de Deus, vamos deixar isso na internet? Obviamente que não. O que mais espanta são as pessoas que ficam encontrando esse tipo de situação – realmente não têm o que fazer. Por isso, a cautela com a privacidade e a intimidade

tem que ser maior.

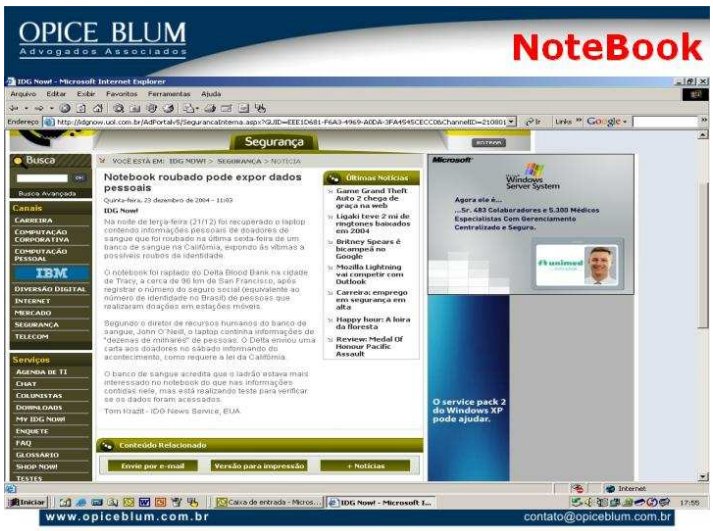
Dois jovens de 19 anos, namorados, tiraram algumas fotos um pouco mais íntimas e guardaram-nas no computador. Depois de um tempo, mandaram o computador para o conserto. No dia seguinte, aquelas fotos estavam na internet também. A cautela tem que existir, inclusive com celular, porque, hoje em dia, tudo é filmado, é monitorado. Cumpre ao Poder Judiciário, quando enfrentar situações como essa, saber indenizar de uma forma pertinente, remover de uma forma pertinente, porque só com decisões judiciais teremos uma força um pouco maior.



Uma decisão bem interessante sobre monitoramento de vias públicas. O criminoso alegou violação à sua privacidade e intimidade diante da prova do crime, que era o monitoramento de vias públicas. E o juiz se manifesta, mais do que corretamente: saber que está sendo filmado não desperta nenhuma indignação, até porque isso de há muito está incorporado no cotidiano das pessoas. Evidentemente que não é o caso. Quem está em ambiente público está ciente que dele se espera um comportamento compatível com a vida em grupo. A restrição da intimidade ocorre no simples fato de as pessoas estarem num local público, e não pelas imagens que a câmera possa captar naqueles locais.

Temos que tomar muito cuidado, também, com as informações que colocamos na internet. Muitas vezes, isso pode ser

utilizado pelos criminosos para a prática de ilícitos. Às vezes, deixamos a nossa intimidade e privacidade de lado, exteriorizando. Por exemplo, o *twitter* é um serviço fantástico, repito, mas tem que ser utilizado com certa cautela. Não é prudente escrever certas coisas: agora estou dando uma palestra no STJ; agora estou indo almoçar com um colega em Brasília; agora estou nesse local. E se alguém quiser lhe prejudicar? É possível encontrar a pessoa a qualquer tempo. Criminosos usam informações da *web* para ameaçar internautas.



Notebook roubado pode expor dados pessoais. Ter aquela segurança da privacidade e da intimidade dentro do *notebook*, criptografia de dados, ou então não guardar dados importantes, como esse caso que mencionei que o casal tirou fotos íntimas e mandou o computador para o conserto.

Quantos computadores novos compramos a cada ano ou a cada três anos? E o antigo, para onde foi? E o que tinha nele? E no *pen drive*? E no celular? E na máquina digital? Cada vez mais, menores dispositivos armazenam mais dados. E tudo isso envolve a privacidade e a intimidade.

Homem tem casa roubada após informar no *twitter* que estava de férias. Vou sair de férias – atenção bandidos. Esse tipo de cautela tem que ser tomada, porque, realmente, tudo isso acontece.

Assim como teve outro caso, em que uma pessoa colocou no *twitter* que estava fazendo uma festa e, de repente, muitas pessoas começaram a chegar à sua casa, obviamente, nem todos conseguiram entrar e houve várias brigas em razão de tudo aquilo.

Ainda dentro da privacidade, vamos fazer uma colisão de direitos em relação ao direito de propriedade. De um lado, temos a privacidade e a intimidade; de outro, temos o direito à propriedade. Aqui, entro no Direito Empresarial.

Resumindo, dentro desses princípios constitucionais: o *e-mail* corporativo ou institucional pode ser monitorado ou não? Por que não poderia? Por que a Constituição garante a inviolabilidade da intimidade e da privacidade? Então, temos um peso muito grande na balança. Temos que colocar outras questões na balança que permitam isso.

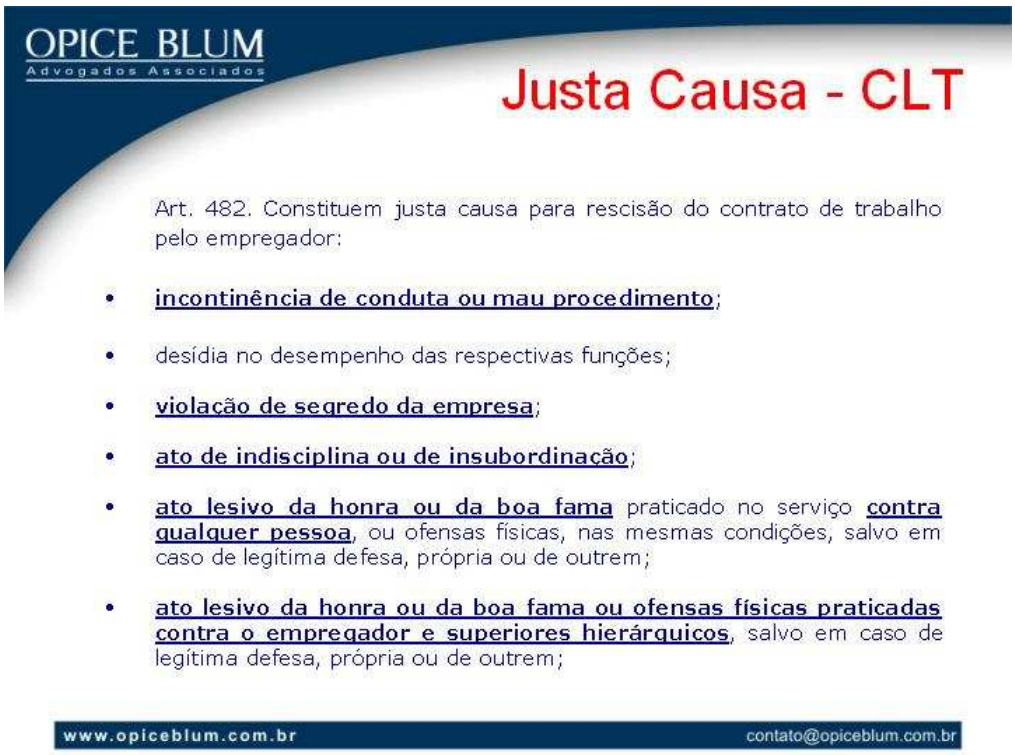
Primeiro, o *e-mail* é para o trabalho e não para a vida pessoal, ou seja, retira-se a expectativa de privacidade; segundo – falando do lado da entidade privada –, a empresa responde pelos atos dos seus funcionários. Quando, normalmente, alguém fala por um *e-mail*, é a empresa que está falando e não um funcionário.

Risco de responsabilidade civil – tem que monitorar. A imagem da empresa – repito que quem está falando é a empresa e não o funcionário; se alguém comete algum ato ilícito, como enviar fotos pornográficas

através do *e-mail* corporativo, é a imagem da empresa que está em jogo, temos que monitorar. Risco de vazamento de informação: concorrência desleal e violação de segredo – mais um motivo.

Colocando na balança essa colisão de direitos, as decisões no Brasil já vêm se pacificando no sentido de que se pode monitorar o *e-mail* corporativo ou institucional, sendo de suma importância que haja um regulamento de segurança específico dando ciência aos funcionários sobre isso.

Só mais um detalhe. Existe a questão do abuso da utilização da internet, ou seja, muitas vezes se monitora para se saber sobre a produtividade, que é mais importante. Poder de direção, previsto no art. 2º da CLT.

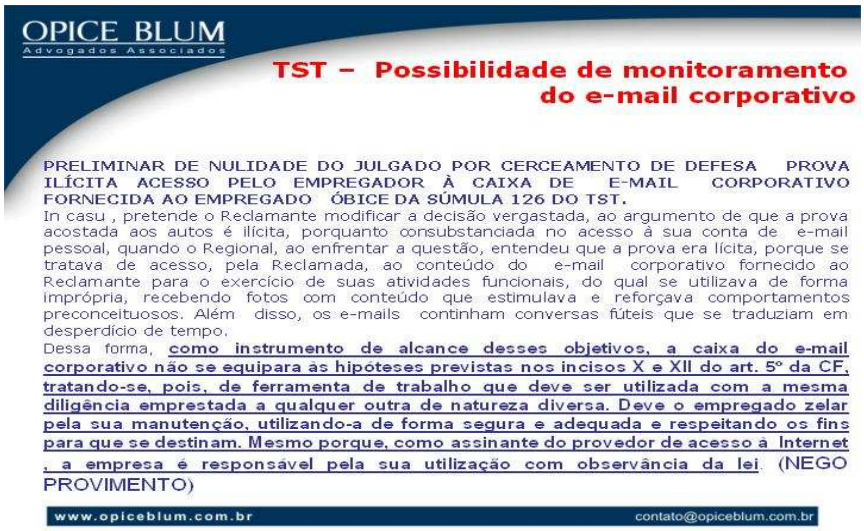


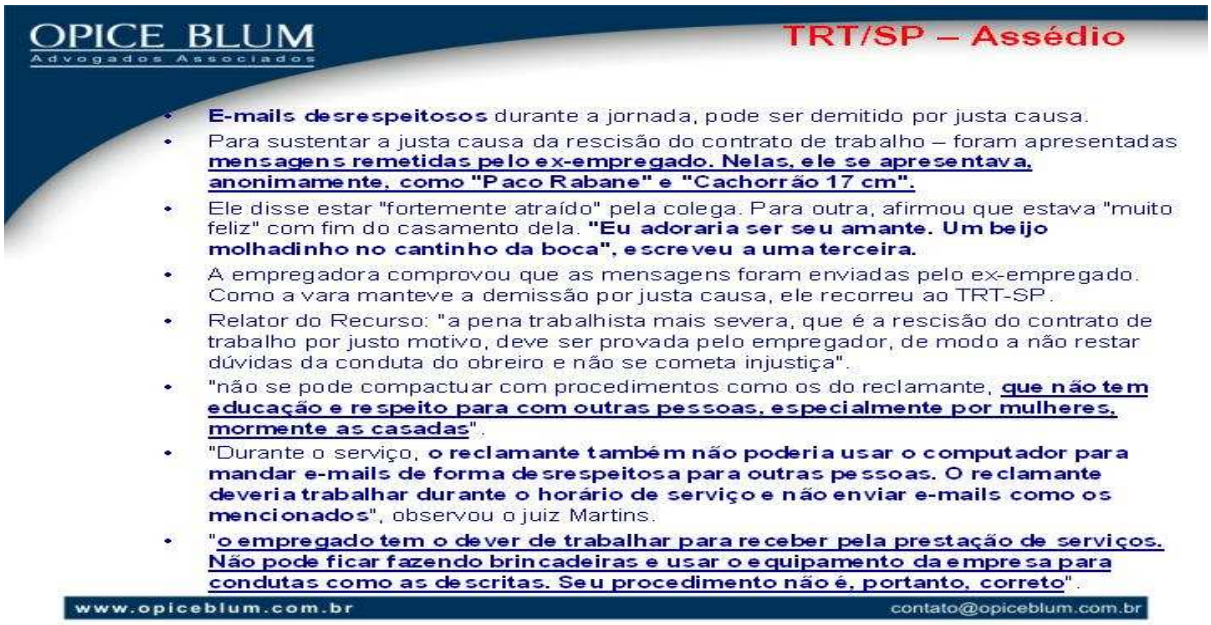
Hipóteses de justa causa. Trago essas hipóteses de justa causa, porque essas decisões são todas da Justiça do Trabalho. Normalmente um funcionário que é demitido por justa causa, em razão de uma prova de um *e-mail* corporativo, alega a nulidade daquela prova, porque estava sendo monitorado e, no mérito, alega que aquilo não é motivo para justa causa.

Essa decisão do Tribunal Superior do Trabalho é de 2004, se não me engano. Até essa decisão, na última instância da Justiça do Trabalho, existiam somente três decisões em Segunda Instância sobre o monitoramento de *e-mail* corporativo. Estavam dois votos a um, contrários ao monitoramento. Veio essa decisão judicial e praticamente pacificou o assunto. Nesse caso, foi enviado um *e-mail* pornográfico, e o funcionário foi demitido por justa causa por incontinência de conduta. Ele alegava que a prova era ilícita, porque contrariava o art. 5º, inciso X, da Constituição.

Decisão do Tribunal Superior do Trabalho: somente o *e-mail* pessoal é passível da proteção constitucional, porque no *e-mail* corporativo são utilizados o terminal de computador da empresa, o provedor da empresa e o endereço eletrônico da empresa. É ferramenta de trabalho para a consecução do serviço. Nesse caso, houve desvio de finalidade, que foi a utilização abusiva e ilegal. Possibilidade de prejuízo ao empregador, dano à imagem e responsabilidade do empregador sobre os seus atos (Código Civil, art. 932, inciso III). Propriedade sobre o computador e provedor, ou seja, outro direito constitucional. De quem é aquele computador, aquele *desktop*, aquele celular, aquele acesso à internet ou aqueles documentos? Da empresa. Finalmente, concluindo que a prova não é ilícita.

Depois, as decisões são contínuas nesse sentido. Também do Tribunal Superior do Trabalho: como instrumento de alcance, não se cogita a hipótese do art. 5º, inciso X, privacidade e intimidade, e nem a do inciso XII da Constituição, inviolabilidade das comunicações, tratando-se, pois, de ferramenta de trabalho. Ou seja, no mesmo sentido.





Às vezes, há uns mais picantes. Nesse caso, o empregado se dirigia às outras pessoas como "Paco Rabanne", e "Cachorrão 17 cm". São impressionantes os casos que existem. Aconteceu no TRT de São Paulo.

O Desembargador de São Paulo assim se manifestou: não se pode compactuar com procedimentos como os do reclamante, que não tem educação e respeito para com outras pessoas, especialmente por mulheres, mormente as casadas. Durante o serviço, o reclamante também não poderia usar o computador para mandar *e-mails* de forma

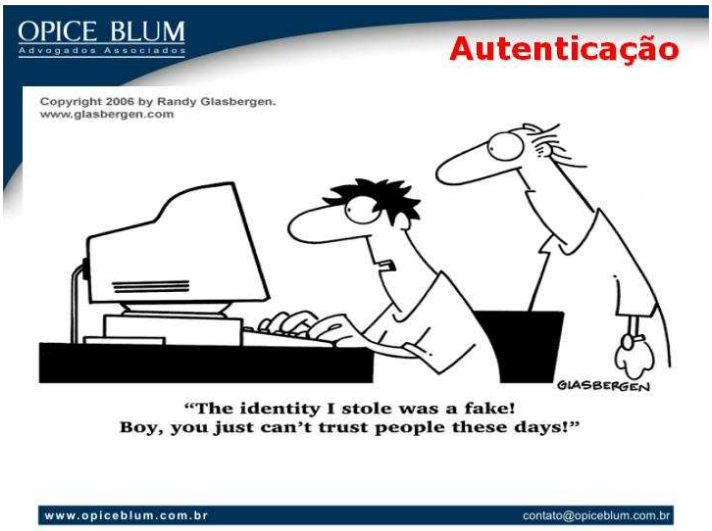
desrespeitosa para outras pessoas. O reclamante deveria trabalhar durante o horário de serviço e não enviar *e-mails* como os mencionados. O empregado tem o dever de trabalhar para receber pela prestação de serviços. Não pode ficar fazendo brincadeiras e usar o equipamento da empresa para condutas como as descritas.

Decisão judicial – disponibilizarei essas aulas para todos os participantes – que mostra a importância do regulamento de segurança. Nesse caso, o Tribunal segue todo o regulamento para concluir que não há interceptação de *e-mails* e não há violação à privacidade nem à intimidade. Bem interessante essa decisão.

A importância do que se chama de Plano Estratégico de Segurança da Informação, que é justamente esse regulamento interno, e a questão da educação e conscientização. Se o órgão faz um

regulamento interno da segurança da informação, mostra transparência a seus funcionários, conscientiza, educa e inibe condutas, porque os funcionários saberão do monitoramento, além de facilitar a prova quando eventualmente seja necessária a utilização.

Art. 5º, inciso IV, da Constituição: É livre a manifestação de pensamento, sendo vedado o anonimato. Talvez as pessoas se esqueçam, muitas vezes, do inciso IV, porque as pessoas dizem "a internet que eu furtei era falsa. Não podemos mais confiar em ninguém nesses dias".



Há uma charge que mostra bem isso: alguém utilizando uma falsa identidade e alguém que já estava utilizando uma falsa identidade. Ou seja, quem está atrás do computador exercendo a manifestação da vontade?

Normalmente, quando pensamos em uma autenticação, em uma senha – somos uma senha quando acessamos o computador, *login* e senha. Daí a importância de não a

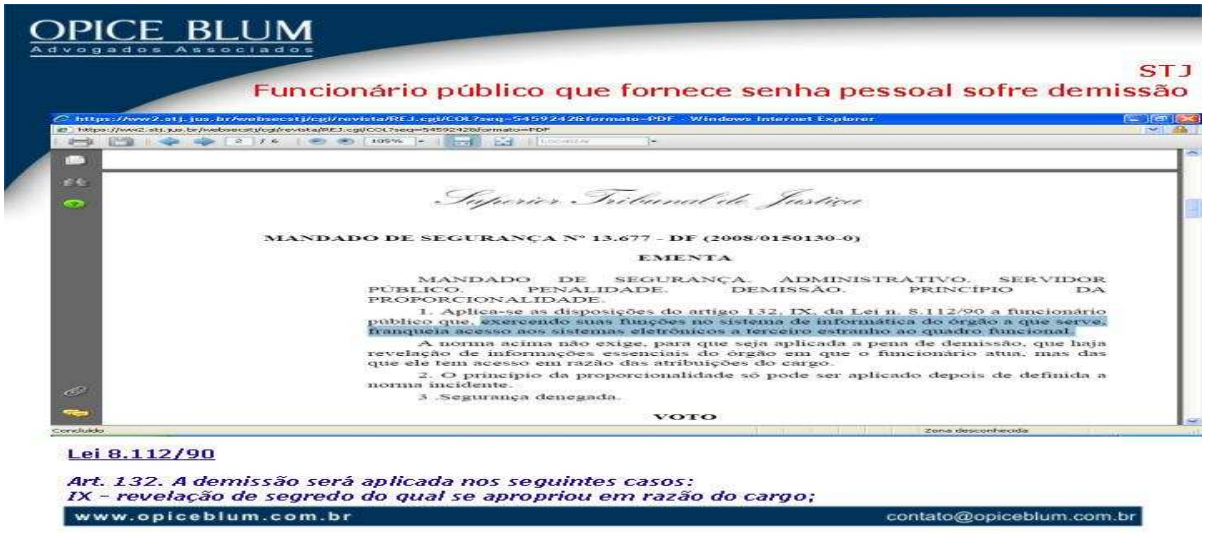
passarmos para terceiros, porque alguém pode se passar por nós – qual objeto vem à nossa mente? Cadeado, o mais comum.

Chave.

Este é um pouco mais eletrônico, uma maçaneta com código.

Este é um pouco mais rústico, um cofre, mais antigo.

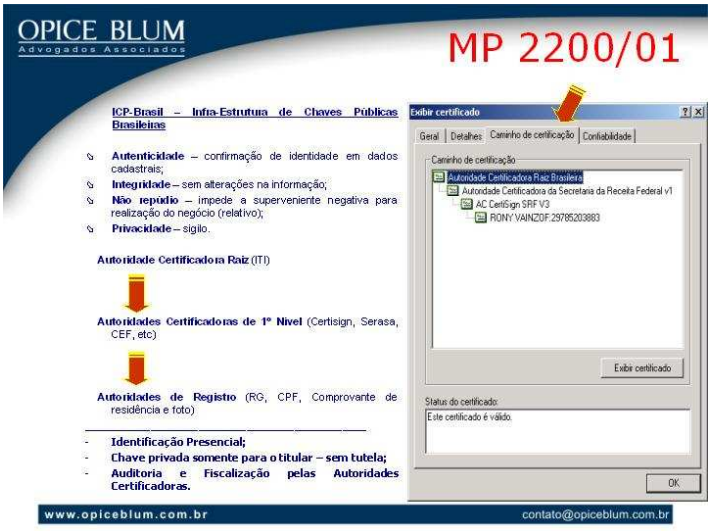
E o que os senhores acham deste? Escova de dentes? É uma chave tecnológica que não estamos conseguindo enxergar? Simples: os senhores emprestam a escova de dentes para alguém? Acho que não. E se alguém a utilizar? É feita a troca, não é?



Questões de conscientização como essas ficam na cabeça em relação à senha. E a senha é tão importante que, por exemplo, em um caso, envolvendo a Administração Pública, um funcionário que forneceu sua senha pessoal sofreu demissão. E essa decisão foi mantida. Aplicam-se os dispositivos da Lei do Funcionário Público àquele que, exercendo suas funções no sistema de informática do órgão a que serve, franqueia acesso aos sistemas eletrônicos a terceiro estranho ao quadro funcional. Essa questão dentro no funcionalismo público é tão importante que é crime.

Art. 325, § 1º, inciso I, do Código Penal – Violação de Sigilo Funcional: aquele que permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública. É crime.

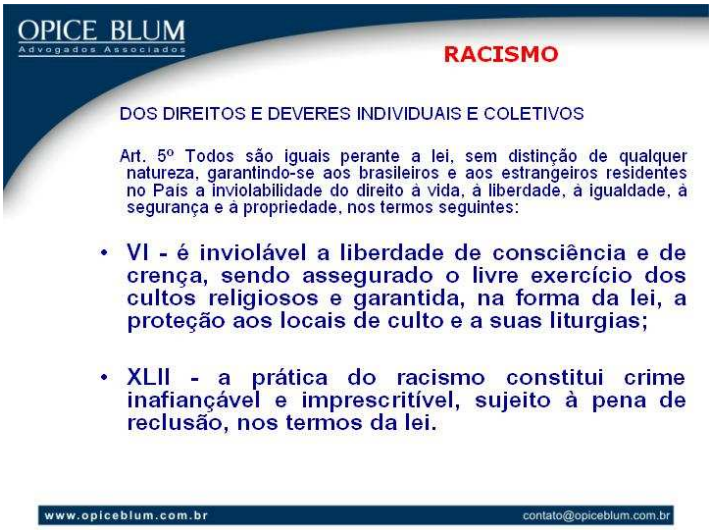
Por isso, temos a Medida Provisória nº 2.200, de 2001, sobre a qual já comentei, que é a ICP – Brasil. Ou seja, a comprovação jurídica de que somos nós mesmos que estamos atrás do computador vem através da assinatura digital.



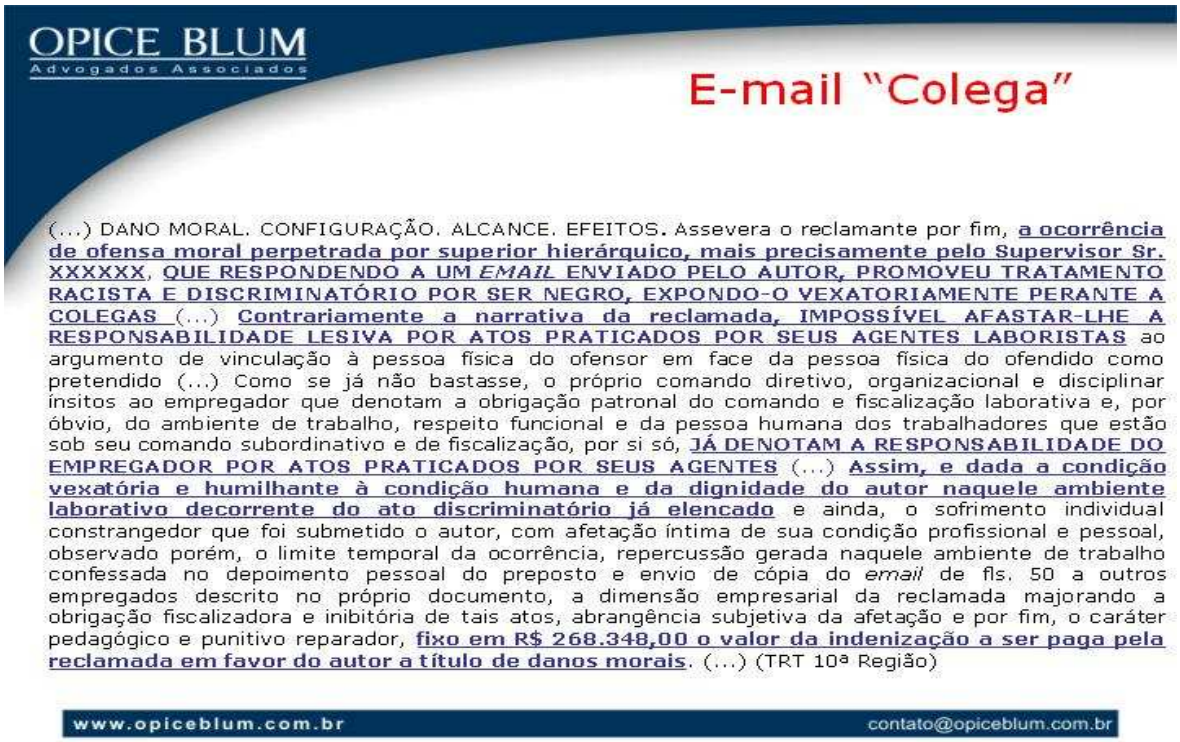
Somente para explicar rapidamente, este é o meu certificado digital, por exemplo, um e-CPF, ou seja, tenho que colocar o meu certificado no cartão da leitora, colocar minha senha, e terei um dispositivo físico mais a senha para que ninguém possa se passar por mim.

Falando sobre a questão de manifestação de pensamento e da liberdade de expressão, há uma colisão de diversos direitos: liberdade de opinião, liberdade de comunicação, liberdade religiosa, liberdade de expressão intelectual, artística e científica, todos esses princípios constitucionais. Com relação aos direitos da personalidade: honra, privacidade, imagem e segurança. Enfim, quem está certo, quem está errado e o que fica ou não no ar? Surgem todas essas questões.

Vimos diversos exemplos de privacidade, de intimidade, de lesão à honra e, principalmente, de anonimato. Nesses casos, deve haver um direito que prevaleça sobre outro direito, principalmente em âmbito constitucional. Então, normalmente o juiz já vem aplicando corretamente essa interpretação constitucional, removendo o que tem que ser removido e indenizando quem deve ser indenizado.



Racismo. Infelizmente, muito comum não somente na internet como um todo, mas, às vezes, dentro da própria empresa.



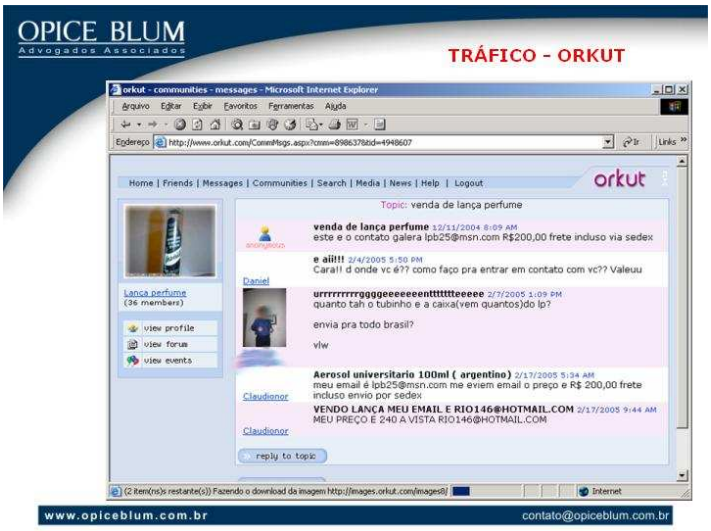
Este caso é de um colega que praticava racismo perante outros colegas através dos *e-mails* corporativos.

Tráfico de entorpecentes, também previsto na Constituição. Fazendo uma pesquisa nesse portal de relacionamentos sobre o lança-perfume,

encontrar-se-á "essa é a comunidade pra quem quer fazer comércio do produto".

Entrando nos tópicos, "quanto está o tubinho e a caixa vem quantos? Envia para todo o Brasil?"

Navegando um pouco mais, percebe-se que a informação é verdadeira, porque têm fotos com colegas, família, mensagens, o que poderá ser utilizado como prova. Daqui a pouco mostrarei algumas provas interessantes.



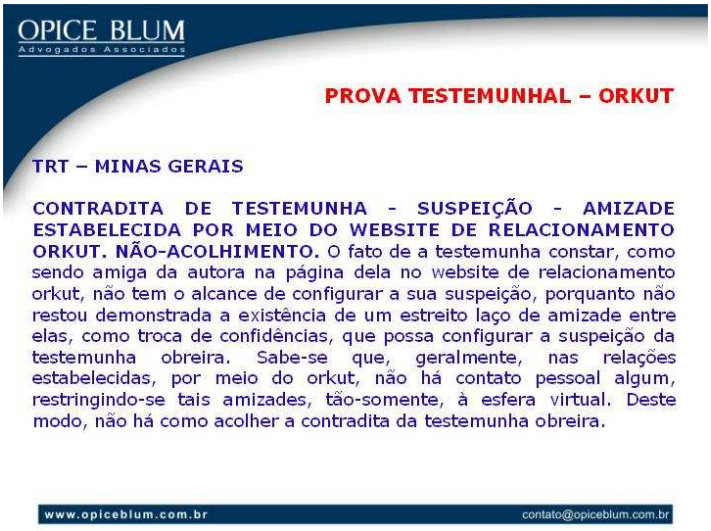
Materialidade do ilícito e a Constituição – provas em geral: aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e a ampla defesa. São inadmissíveis no processo as provas obtidas por meios ilícitos. Essa é uma cautela que se deve ter em uma investigação eletrônica para não caracterizar uma prova obtida por meio ilícito.

Outra charge bastante interessante: "seu raio X mostrou uma costela

quebrada, mas não se preocupe, porque a corrigimos no *photoshop"*. Imaginem que o sujeito está com um problema no mundo físico, com uma costela quebrada, e que esse médico tenha se formado em uma nova universidade, onde ensinam como se operar costelas através do *photoshop* e que aquilo seja válido pela medicina. O sujeito está com problema no mundo físico, mas não consegue comprovar que está com esse problema, porque no mundo eletrônico isso já foi sanado – obviamente que nesse caso é impossível – mas e em outros casos?

O que é certo ou errado? Espera-se sempre que o bem prevaleça sobre o mal. Teve um caso envolvendo pornografia infantil em que o pedófilo – não é mais adequado falar-se pedófilo, porque pedofilia é a doença; quando se fala de doente, pode ter alguma proteção dos advogados para que o cliente não seja condenado –, ou melhor, o criminoso mascarava o próprio rosto usando o *photoshop*. Os peritos fizeram uma engenharia reversa, conseguindo identificar exatamente a face dele, o que culminou na sua prisão.

Outro exemplo: antes de ir a uma audiência, um colega advogado pesquisou em um *site* de relacionamento quem era a testemunha para contraditá-la. Não deu certo, não por causa da prova eletrônica. Vejam a conclusão do juiz: amizade estabelecida por meio do *website* de relacionamento. O fato de a testemunha constar como sendo amiga da autora na página dela no *website* de relacionamento, não tem o alcance de configurar a sua suspeição, porquanto não restou demonstrada a existência de um estreito laço de amizade entre elas, como troca de confidências, que possa configurar a suspeição da



testemunha obreira. Sabe-se que, geralmente, nas relações estabelecidas por meio do *site* de relacionamentos não há contato pessoal algum, restringindo-se tais amizades, tão-somente, à esfera virtual. Ou seja, como é um amigo virtual e não um amigo físico, não poderá ser declarada a suspeição, a contradita da testemunha.

Outro caso envolvendo justiça gratuita. A parte entrou com pedido de justiça gratuita. O juiz abriu para a parte contrária, que impugnou a justiça gratuita. Para impugnar, acessou o *site* de relacionamento da autora e viu fotos que demonstravam que, pelo menos, três vezes ao ano aquela pessoa viajava para Europa. Juntou essas provas aos autos, e o juiz alegou que quem viaja três vezes ao ano para Europa pode arcar com as custas do processo.

Brinco ou *pen drive*? Os dois. O *pen drive* em forma de brinco facilita a obtenção de provas extraídas de um computador de um funcionário suspeito. Quantos formatos pode ter um *pen drive?* Pode ter um formato de brinco, de chaveiro ou de caneta.

Onde estão as provas? Essa é uma grande questão. Os peritos têm que saber onde estão as provas. Repito que cada vez mais os menores dispositivos armazenam mais dados. Esse é um grande risco.

Rastreador do ar. Esse adaptador permite a interceptação de tudo que trafega via W*i-Fi* ou W*iMax*?

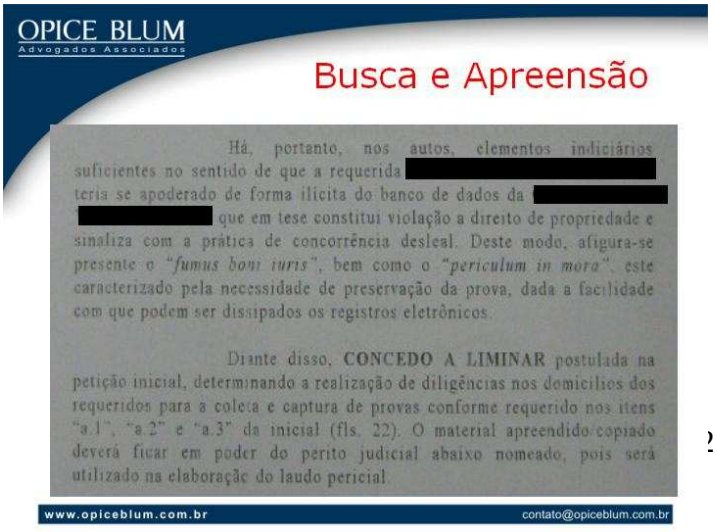
Interceptação de dados telemáticos ou informáticos. Crime: *ipod* espião. Nesse caso, em menos de dois minutos, ele consegue fazer a clonagem de um HD.

Enfim, dentro da tecnologia, tudo pode ser feito. Por isso, devemos tomar cuidado para que seja feito dentro da mais pura legalidade, para não haver discussão sobre as provas.

Art. 5º, inciso XI, da Constituição, sobre a inviolabilidade do domicílio, a não ser com ordem judicial. A grande maioria dos ilícitos eletrônicos envolve busca e apreensão, porque somente através do recolhimento do material utilizado na prática de ilícitos é possível se comprovar principalmente a autoria, porque, muitas vezes, a materialidade já está comprovada.

Normalmente, temos uma busca e apreensão, que terá um objeto de exame pericial, e, aí sim, a prova do direito à ação, seja a parte, se for uma ação penal privada ou uma ação civil, seja o Ministério Público, se for uma ação pública.

Exemplo de liminar de busca e apreensão deferida – está um pouco escuro, mas é só um exemplo prático. O material apreendido/copiado deverá ficar em poder do perito

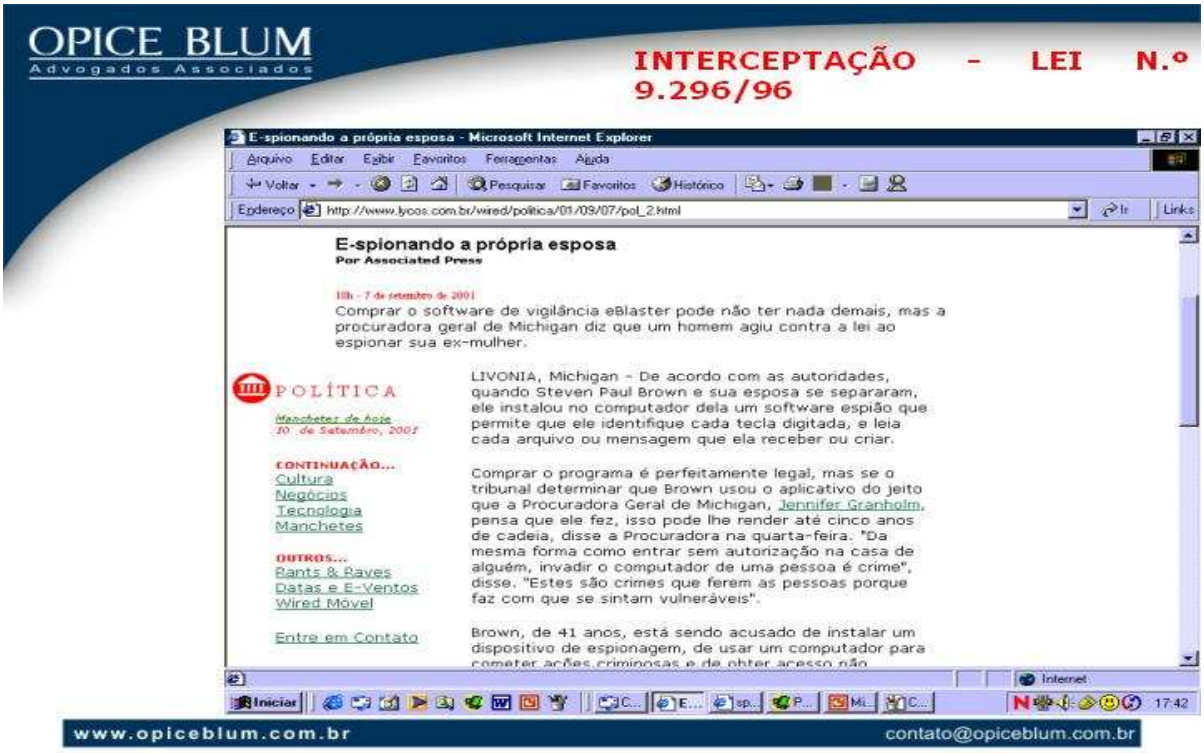


judicial, pois será utilizado na elaboração do laudo pericial. Trata-se somente de apresentar os requisitos, deferindo a busca e apreensão.

Por isso, temos que saber onde estão as provas. Trago alguns exemplos: *desktops*, *notebooks*, HDs externos. O HD externo ligado a uma porta USB tem mais de um *terabyte* de informação normalmente. Um *terabyte* de informação é um mundo de informações. O custo de um HD externo, hoje, é em torno de cento e cinquenta dólares. Pode-se carregar uma companhia inteira na palma da sua mão. Os criminosos também podem carregar as provas dos ilícitos através disso. Deve-se ter a cautela de identificar onde está a prova dos ilícitos: câmeras digitais, servidores, *smartphones*, celulares, aparelhos de MP3, dentre outros.

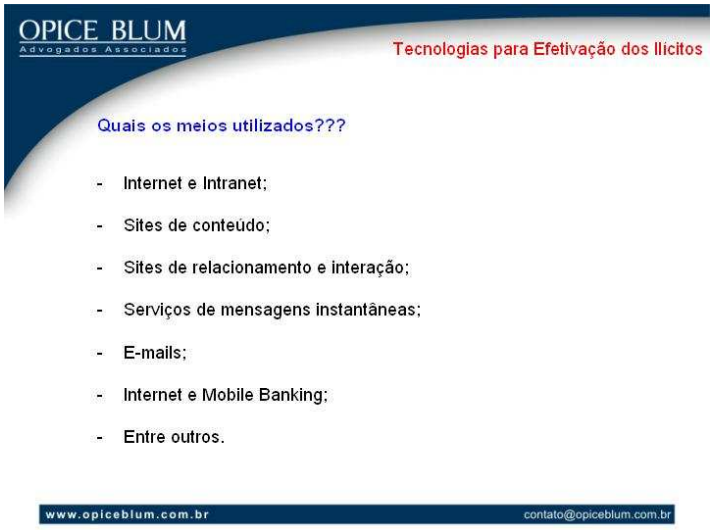
É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas – art. 5º, inciso XII.

A Lei nº 9.296/96 regulamenta. Art. 1º, parágrafo único: o disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática ou telemática. É crime realizar a interceptação de comunicação telefônica, de informática ou telemática.



O que é interceptação? Darei um exemplo que aconteceu nos Estados Unidos: de acordo com as autoridades, quando Steven Paul e sua esposa se separaram, ele instalou no computador dela um *software* espião, que permite que ele identifique cada tecla digitada e leia cada arquivo ou mensagem que ela receber ou criar. Obviamente, esse não é o exercício regular de direito de um ex-marido. O que é isso? É o chamado *spyware*. Ele instalou o *software* e saberá tudo que for digitado. Isso é interceptação. É daqui para o futuro. A pessoa passa a interceptar. É o

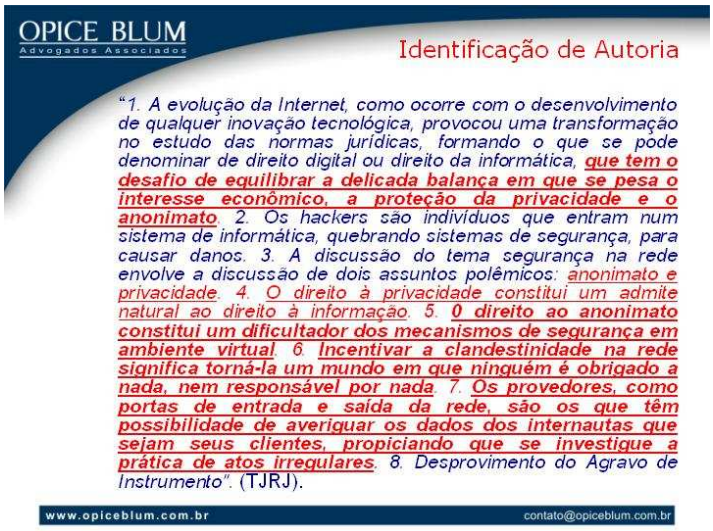
fluxo e não dados estáticos.



Dentro dessa questão de interceptação, quais os meios utilizados para justamente saber em que caso se pode solicitar essa interceptação de forma correta? Internet ou intranet – às vezes está dentro da empresa e não na grande rede mundial de computadores; s*ites* de conteúdo? SMS?

Caso ocorrido em Portugal. Um sujeito foi abordado pela autoridade policial que viu que ele estava com um celular. Havia um SMS com o seguinte texto: "a droga que você ia vender por 10, venda por 100". Entrou na discussão se a prova era lícita ou ilícita. Imaginem essa situação no Brasil. Seria lícito ou ilícito? Essa prova seria válida ou não? Não é a mesma coisa de alguém andar com um papel dobrado dentro do bolso e ser revistado? Quando o policial tem fundada suspeita, ele pode fazer uma revista íntima. Se os celulares tivessem senha, porque não poderia?

Quebra de sigilo do IP. Quando se pede a quebra de sigilo de um IP para identificar os dados cadastrais do responsável por determinada conduta ilícita, não é um pedido de interceptação, art. 5º, inciso XII, da Constituição, e sim um mero pedido de dados cadastrais, ou seja, os dados estão estáticos no provedor. A interceptação é fluxo daqui para o futuro. Por exemplo, está tendo uma fraude no *internet banking*. Preciso que o provedor me informe tudo o que está trafegando na rede daquele fraudador, daqui para frente. Isso é interceptação.



Exemplo de quebra de sigilo de IP. Vejam que interessante essa decisão judicial e como os juízes já têm conhecimento da matéria. O direito ao anonimato constitui um dificultador dos mecanismos de segurança em ambiente virtual. Incentivar a clandestinidade na rede significa torná-la um mundo em que ninguém é obrigado a nada, nem responsável por nada. Os provedores, como portas de entrada e saída da rede, são os que têm possibilidade de averiguar os dados dos internautas que sejam seus clientes, propiciando que se investigue a prática de atos irregulares. Liminar deferida.

Senhores, por enquanto, só tenho a agradecer. Terei a felicidade de estar aqui no começo da tarde. Espero que tenham gostado.

Muito obrigado.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Boa tarde a todos. Retornamos com as palestras do Seminário de Direito Eletrônico, uma iniciativa do STJ e do Instituto dos Magistrados do Distrito Federal (Imag-DF).

Nesta segunda parte, voltamos com o Dr. Rony Vainzof, que falará sobre a Responsabilidade Civil na Informática. Repetiremos o currículo do Dr. Rony Vainzof em razão de termos participantes que não presenciaram a palestra matutina.

O Dr. Rony Vainzof é sócio do Opice Blum **-** Advogados Associados. Graduado pela Faculdade de Direito da Universidade Presbiteriana Mackenzie e Pós-Graduado em Direito Processual Penal pela mesma Universidade; Coordenador, Assistente e Professor do MBA em Direito Eletrônico da Escola Paulista de Direito (EPD); Professor convidado da Fundação Getúlio Vargas e da Universidade Presbiteriana Mackenzie nos cursos de Pós-Graduação em Direito Digital e das Telecomunicações, bem como Computação Forense; Professor das Faculdades FIAP, IBTA, UNIGRAN, UNICID, UNISA e do Instituto Paulista de Educação Continuada. É, ainda, Vice-Presidente do Conselho Superior de Tecnologia da Informação da Federação do Comércio do Estado de São Paulo e Vice-Presidente do Comitê de Direito de Tecnologia da Câmara Americana do Comércio (AMCHAM).

A participação está aberta a todos. Caso queiram fazer perguntas, levante a mão que levaremos o microfone.

Com a palavra o Dr. Rony Vainzof.

PALESTRA III: RESPONSABILIDADE CIVIL NA INFORMÁTICA

RONY VAINZOF
Professor do MBA em Direito Eletrônico da Escola Paulista de Direito

Boa tarde a todos.

Anteriormente falamos sobre as questões constitucionais e vimos que, apesar de não existir muita legislação específica sobre o direito eletrônico, existe muita legislação aplicável sobre esse assunto. Seguiremos com essa trajetória, dentro da responsabilidade civil, e verificaremos como aplicar o Código de Defesa Civil e o Código de Defesa do Consumidor e demais ordenamentos jurídicos civis em relação a essas novas tecnologias.

Mencionei para os senhores alguns casos relacionados à responsabilidade. Falei um pouco sobre as indenizações, porque não há como deixar de aplicar o Direito Constitucional sem vincular diretamente a todas as situações práticas relacionadas a todas as áreas do Direito: Direito Civil, Direito Penal, Direito Tributário, Direito Trabalhista, Direitos Autorais. Agora, especificaremos alguns pontos, e alguns *cases* relacionados ao Direito Civil.

Uma grande situação, muito questionada em relação ao Direito Civil, está relacionada à responsabilidade dos provedores de conteúdo, de uma forma geral.

Citando como exemplos de provedores de conteúdo, aquele que provê o conteúdo na internet, temos os *sites* de jornais, as televisões, os *sites* de relacionamentos e os *blogs.*

Qual seria a grande responsabilidade desses provedores de conteúdo? Será que eles teriam a responsabilidade objetiva prevista no parágrafo único do art. 927 do Código Civil? Será que eles teriam a responsabilidade subjetiva prevista no art. 186 do Código Civil, que dispõe: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."? Qual seria o tipo de responsabilidade a ser aplicada? Se aplicarmos uma responsabilidade objetiva pelo risco da atividade, por exemplo, será que não estaríamos dizendo que esses provedores de conteúdo teriam uma obrigação prévia de verificar o conteúdo que estão hospedando para somente depois divulgá-los? Será que isso não seria uma censura prévia em relação a tudo isso?

Um caso bastante famoso foi publicado em um jornal físico, jornal escrito. Tratava-se de uma informação acerca da condenação de uma determinada pessoa. Um portal jurídico leu essa matéria, considerou-a interessante e a publicou também. Esse portal jurídico, por sua vez, é hospedado por um grande provedor de acesso e conteúdo à internet, como, por exemplo, Terra, UOL, entre outros. Ou seja, neste caso temos três envolvidos: o jornal físico que fez e publicou a matéria; o portal jurídico que a considerou interessante e fez o *upload* dessa matéria; e o provedor de hospedagem, que é um grande provedor e tem a hospedagem daquele portal jurídico.

Porém, aquela matéria divulgada era indevida, porque não havia nenhuma condenação criminal contra aquela pessoa. Então, surgiu um ato ilícito passível de indenização. Neste caso, trata-se de indenização por danos morais. A grande questão é: quem, dos três, seria responsável civilmente por isso? O jornal, que publicou a matéria; o portal jurídico que a considerou interessante e fez o *upload*; ou o provedor de hospedagem que hospedava aquele portal jurídico? O que os senhores pensam? Quem

seria o grande responsável? Seriam os três, nenhum dos três, dois deles ou não?

Comecemos a análise pelo mais simples. O jornal escrito, que fez e publicou essa matéria, parece-nos que é responsável. E o portal jurídico, seria responsável ou não? Levantem a mão, por favor, quem julga que o portal seria responsável. *Quorum* mínimo aqui? Agora, quem considera que o portal jurídico não seria responsável? Há várias pessoas que não responderam, pois estão em dúvida ainda.

O portal jurídico que publicou o material seria responsável porque deveria checar a veracidade das informações, ou seja, após ter identificado aquela matéria, considerou-a interessante, imaginou que daria mídia e a publicou. Porém, não confirmou se aquela matéria seria verdadeira ou não. Mas, como o colega disse aqui, citou a fonte. Ao citar a fonte, ele não estaria isento de responsabilidade? Na minha opinião, não porque houve um juízo de valor para colocar aquela matéria no ar, mas, mesmo assim, sem verificar a veracidade daquela matéria, ela foi publicada.

E o provedor de hospedagem, que está hospedando esse portal, por exemplo, um Terra, um UOL ou um IG, teria responsabilidade? O que os senhores pensam? Os senhores julgam que o provedor de hospedagem, que hospeda milhares de *bits* e *bytes* de informação, tem obrigação de verificar todo o conteúdo que está sendo divulgado através deles? Por exemplo, aqueles *sites* de leilão na internet, cuja responsabilidade está vinculada à aproximação de compradores e vendedores, que não são lojas virtuais, respondem pelo Código de Defesa do Consumidor, porém, o seu serviço é aproximar compradores e vendedores e não, exatamente, vender o produto.

Os senhores julgam que esses *sites* teriam responsabilidade em relação aos produtos que estão sendo vendidos pelos usuários da internet como um todo? Se assim fosse, em uma seção de relógios que estão sendo vendidos no *site,* precisaria ter um especialista em relógios para

saber se esses produtos seriam contrafeitos ou não. Em relação aos carros, o *site* teria que verificar se estes seriam produtos de receptação ou não; e assim por diante para todos os produtos relacionados à internet, o que inviabilizaria o negócio propriamente dito, assim como acontece no caso desse grande provedor de hospedagem. É inviável, tecnicamente, que ele verifique tudo o que está sendo divulgado, simplesmente porque isso poderia caracterizar uma censura prévia, contrária, inclusive, à nossa Constituição.

Por isso que, neste caso, seriam responsáveis – e essa foi a decisão judicial – o jornal que publicou a matéria, bem como o provedor de hospedagem, que fez o juízo de valor e hospedou a matéria.

Os senhores podem me perguntar se o portal, que está hospedando, nunca seria responsável por isso. Responsabilidade objetiva, ele não tem. Se a pessoa que não foi condenada quiser tirar aquela matéria do ar, por ser indevida, deve dirigir-se ao provedor e dizer: "Senhor provedor, o senhor hospeda um portal jurídico que está divulgando uma matéria de conteúdo indevido. Por favor, remova, imediatamente, essa matéria do ar."

Provedor de hospedagem não tem uma obrigação de monitoramento prévio, porém, a partir do momento que toma conhecimento de um ato indevido, se não remover a matéria do ar, responderá pela responsabilidade subjetiva prevista no art. 186 do Código Civil, pois passou a ser negligente; foi omisso, mesmo sabendo de um ato ilícito. A partir desse momento, então, ele passa a ser responsável.

Apresentarei para os senhores diversas decisões nesse sentido e algumas outras decisões, inclusive uma do STJ desta semana, dispondo acerca da manutenção de uma multa contra um *site* de relacionamento na internet que não retirou algumas matérias ofensivas do ar. É bastante interessante.

A responsabilidade civil não se aplica somente em relação aos provedores em si. Temos que falar sobre a responsabilidade que nós, usuários comuns, temos em relação à internet como um todo. Cada vez mais é crescente aquele conceito de homem comum para que o juiz analise, no momento de julgar uma ação, o conhecimento das novas tecnologias e a obrigação de que, atualmente, os usuários devem ter um razoável conhecimento sobre a vulnerabilidade dos seus sistemas. Isso serve, principalmente, para os pais em relação aos filhos, porque no art. 932 do Código Civil, inciso III, consta a responsabilidade da empresa sobre os seus funcionários, também consta a responsabilidade dos pais pelos filhos menores no inciso I.

Comentando um pouco acerca da apresentação feita, hoje, pela manhã. Se fizermos um regulamento de segurança da informação dentro das nossas empresas, dos nossos escritórios, dos nossos órgãos administrativos e deixarmos a segurança da informação juridicamente perfeita, mas sairmos para trabalhar e deixarmos os filhos em casa, com computador, com acesso à *internet*, mas sem segurança, estaremos correndo um grande risco. Devemos ter em casa uma política de segurança da informação e, se o filho não a cumprir, nós o demitiremos por justa causa? O que os senhores pensam? Sabemos que se trata de uma questão de educação e conscientização, porque está cada vez mais comum acontecerem esses atos.

Por exemplo, no caso de um filho menor, que tem certeza absoluta que a professora de Ensino Médio não é mulher, na realidade é um homem, e tira uma foto dela com o celular, cria uma página, faz um bigode no *photoshop* e divulga essa foto em uma página de relacionamento, os responsáveis por isso serão os pais.

Houve um caso em que um garoto com quatorze anos de idade tinha uma namorada também com quatorze anos na escola. Sabemos que, atualmente, os relacionamentos também são virtuais. O garoto estava conversando em um *chat* com a namorada por meio de uma

webcam – invariavelmente, essa sempre é uma ideia dos homens – e resolveram fazer uma brincadeirinha de perguntas e respostas; quem fosse perdendo ia tirando uma peça de roupa. Infelizmente, a garota perdeu o jogo e, no auge da maturidade desse garoto com quatorze anos, congelou duas imagens dela e passou para dois amiguinhos, também com quatorze anos, que, obviamente, no auge de suas maturidades, não passaram para ninguém.

A foto foi divulgada na internet. A menina teve que sair da escola por causa da vergonha que estava passando, um abalo moral fortíssimo; o pai ficou sabendo, levou ao conhecimento da autoridade policial, porque, por bem ou por mal, fotos envolvendo criança ou adolescente na internet configuram crime de pornografia infantil, pelo Estatuto da Criança e do Adolescente, art. 241 e seguintes. O garoto foi chamado pela autoridade policial, junto com o pai obviamente, para prestar depoimento sobre o fato, pois a garota havia indicado que, possivelmente, teria sido ele o responsável pela divulgação. O garoto explicou que somente congelou as fotos, mas que não tinha divulgado para a internet, somente para dois amigos.

O inquérito foi relatado e enviado para a Vara da Infância e da Juventude. O Promotor de Justiça aplicou a medida sócio-educativa de prestar serviços à comunidade carente, ensinando jovens a utilizar, de forma adequada, a internet. Os seus pais foram advertidos. É interessante o fato de que, muitas vezes, a legislação funciona bem, pois o garoto gostou tanto dessa atividade que depois, mesmo voluntariamente, continuou ensinando.

Além disso, imaginem a responsabilidade civil, a lesão moral que essa garota sofreu e, em razão da qual, os pais poderiam sofrer uma indenização. É por isso que, nas escolas, além das universidades, cresce bastante esse tipo de matéria relacionada aos riscos legais na internet dentro de casa. Não é só a questão da responsabilidade civil como um todo, mas principalmente a educação e a conscientização, porque se,

muitas vezes, nós, adultos, não sabemos como lidar com as novas tecnologias sob o aspecto do Direito, imaginem as crianças e os adolescentes que já vivem neste mundo diretamente.

Deixarei com os senhores alguns slides com cartilhas sobre esse assunto, inclusive uma elaborada pelo Ziraldo, que é "A Internet do Menino Maluquinho", bastante interessante; e é bom para as crianças e os adolescentes lerem, porque mostra que existem os riscos.

Algumas dicas sempre são válidas dentro de casa, como não deixar o computador em um lugar fechado, sendo utilizado somente pelo filho; deve sempre estar nos locais em que há circulação de outras pessoa; e, dependendo da idade, os senhores devem sempre acessar a internet junto com seu filho.

Assisti a uma palestra interessante em que o palestrante falou: "em casa o meu filho pode acessar o que quiser, mas tenho um programa de monitoramento que ele sabe que posso ver tudo o que ele for acessar; então, há liberdade plena, mas sei de tudo". Com certeza, dessa forma, os senhores estarão inibindo certas condutas e transmitirão uma educação mais condizente.

Falaremos, agora, sobre os provedores de hospedagem. Mencionei bastante, na primeira apresentação, que a identificação de qualquer tipo de ilícito eletrônico depende de uma informação do provedor de acesso. Retomando esse assunto para quem não estava de manhã, para sabermos quem está atrás do computador, a pessoa precisa assinar um provedor de acesso à internet, mediante um contrato. Normalmente, é por meio do protocolo e do provedor de acesso utilizado que se investiga um crime.

Pergunto: existe alguma legislação específica que obrigue esses provedores de acesso a manterem esses registros eletrônicos? E se eles não mantiverem esses registros eletrônicos, eles deveriam ser responsabilizados pela conduta ilícita do cliente que utilizou aquele acesso ou não? Afinal de contas, pelo princípio da lei, da legalidade e da reserva

legal, ninguém é obrigado a fazer ou deixar de fazer, senão em virtude de lei. Se não há nenhuma lei específica sobre o assunto, por que esses provedores de acesso seriam responsáveis se não conseguirem identificar os autores dos ilícitos?

Houve uma fraude no *internet banking*, no valor de R$ 29.000,00 (vinte e nove mil reais). O banco não quis discutir com o cliente de quem seria a responsabilidade e ressarciu o cliente no valor total da fraude. Porém, o banco queria identificar quem era o fraudador. Assim, buscou, nos seus registros eletrônicos, quem fez aquele acesso ao banco para praticar aquela fraude, ou seja, aquele IP, naquela data e naquele horário. Constatou-se que o provedor de acesso à internet foi por meio de um celular. Prestem bem atenção às datas que vou falar.

Após dez dias da ocorrência da fraude, notificamos o provedor de acesso à internet, comunicando que ocorreu a fraude, que o cliente acusou que não foi ele quem fez essa transferência, que o banco já ressarciu o cliente, mas quer saber quem é o fraudador e solicitando todos os dados. Porém, o provedor não forneceu a informação, extrajudicialmente, pela questão do sigilo, da privacidade e da intimidade. Será que, neste caso, seria essa a situação? Se estamos diante de um ato ilícito, o provedor não poderia fornecer esses dados?

Vamos analisar diante de alguns princípios constitucionais. Art. 5º da Constituição Federal, inciso X, que trata da privacidade e intimidade e inciso XII, que trata da inviolabilidade das comunicações. Lembrando que no inciso XII tem a observação (Vide Lei nº 9.296/1996), que

regulamenta as vedações da interceptação das comunicações telefônicas, informáticas e telemáticas.

Vamos começar pelo mais fácil. Esse pedido para o provedor de acesso não seria um pedido de interceptação de dados, pois estamos solicitando dados cadastrais como: nome, RG, CPF, endereço do responsável por aquele contrato de acesso à internet. São dados cadastrais e informações estáticas que estão preservadas no provedor. Portanto, não precisamos seguir a Lei nº 9.296 e não é necessária uma ordem judicial diante de uma instrução processual penal.

Há outro ponto interessante: falamos em interceptação quando falamos em conversa de terceiros, porque sempre que se participa de uma conversa, não há que se falar em interceptação. Se faz parte da comunicação, não é interceptação.

Será que se aplicaria, neste caso, o inciso X do art. 5º que trata da privacidade e da intimidade? Não estamos perguntando se a pessoa gosta de comer abacaxi ou melão, se torce para o Corinthians ou para o São Paulo, ou se gosta de acessar *site* de *e-commerce* ou *site* de relacionamento. Estamos perguntando sobre os dados cadastrais, e existem diversas decisões judiciais, apesar de ser uma contradição e ter diversas decisões diferentes sobre o fato de que dados cadastrais não estariam protegidos pelo art. 5º, inciso X, da Constituição.

Na prática, os provedores exigem ordem judicial para o fornecimento dessas informações. Neste caso, por que devo notificar, extrajudicialmente, esses provedores? Existe uma questão técnica e outra jurídica. A jurídica é para não ter uma carência da ação e mostrar que houve uma tentativa extrajudicial. E a técnica? Se não sabemos por quanto tempo esses provedores guardam essas informações, na notificação de solicitação do fornecimento dos dados deixaremos claro que, se houver a exigência da ordem judicial, iremos obtê-la, portanto, já determinaremos que esses dados sejam preservados desde já.

Decorridos dez dias da fraude, o banco notificou o provedor para preservar aqueles dados. Cinco dias depois, ou seja, quinze dias após a fraude, o provedor respondeu que somente forneceria aqueles dados mediante uma ordem judicial, o que é um procedimento normal, feito pela esfera cível, porque é muito mais célere do que a esfera criminal. Às vezes, em São Paulo, por exemplo, uma quebra de sigilo como essa, na esfera criminal, pode demorar mais de seis meses, ou seja, esqueça qualquer tipo de investigação.

Na esfera cível, essa quebra de sigilo para fornecimento dos dados, normalmente, ocorre em até 48 horas, mais ou menos. Entra-se com uma ação cível, uma obrigação de fazer com pedido liminar contra o provedor. Para conseguir essa liminar, precisamos dos requisitos jurídicos. Simplificando, fumaça do bom direito, **periculum in mora.** Fumaça do bom direito seria a fraude e a carta de contestação do cliente, falando que não foi ele quem fez aquela transferência, e o comprovante de ressarcimento do banco perante o cliente. O perigo de demora está justamente no risco de o provedor perder esses dados – e a cada dia que passa o fraudador está solto –, então precisamos dessa informação rapidamente.

O juiz deferiu a liminar. No décimo dia após a fraude, notificamos o provedor; no décimo quinto dia após a fraude, o provedor respondeu que somente tomaria as providências mediante uma ordem judicial a qual foi determinada; e no trigésimo primeiro dia após a fraude, o provedor foi intimado judicialmente para prestar as informações. Após mais ou menos dez dias, o provedor responde que, infelizmente, não é possível mais cumprir a ordem judicial, porque esses dados ficam arquivados por trinta dias. Portanto, não foi possível descobrir quem é o fraudador em razão desse ato ilícito; talvez, em outra fraude que ele cometa, com outro banco, com outra vítima.

Então, em uma ação de obrigação de fazer, neste tipo de caso, em que a obrigação não pode ser cumprida, cabe uma conversão da

obrigação não cumprida em perdas e danos, a qual foi solicitada em razão dos danos materiais no valor de R$ 29.000,00 (vinte e nove mil reais); e danos morais, pela sensação de impunidade e pela desestabilização do *internet banking* como um todo em razão desse tipo de conduta.

O provedor respondeu que não existe nenhuma lei específica sobre o assunto; portanto, pelo princípio da legalidade, ele não teria essa obrigação e começou uma discussão jurídica. De fato, não há lei específica. Temos no Brasil, sobre esse tipo de assunto, uma recomendação do Comitê Gestor da Internet, que determina que os provedores devem guardar esses dados pelo prazo de três anos. É uma recomendação; não é uma lei. O projeto de lei aprovado no Senado Federal e na Câmara dos Deputados prevê também esse prazo de três anos.

A fundamentação para a conversão em perdas e danos baseou-se no art. 186 do Código Civil, que trata da responsabilidade subjetiva, e na recomendação acima mencionada. Alegou-se que, no décimo dia, o provedor foi notificado extrajudicialmente, quanto ele tinha os dados; no décimo quinto dia o provedor respondeu que precisava de ordem judicial, quando também ele tinha os dados. No momento em que essa ordem judicial foi deferida, eles não se preocuparam em preservar os dados, respondendo que só guardam essas informações por trinta dias? Quem não quer ser negligente e imprudente cumpre a recomendação do Comitê Gestor da *Internet* que determina que se deve guardar esses dados por três anos, por isso requereu-se a conversão em perdas e danos.

Na audiência de conciliação, estive presente pelo banco, e a parte contrária não compareceu. Enfim, não foi à revelia, porque já tinha respondido, mas, para efeitos práticos, não aceitaria qualquer tipo de composição. Obviamente, eles poderiam ter peticionado anteriormente, com essa informação, ao invés de esperar a audiência.

Tive a oportunidade de conversar sobre este caso com um magistrado que também questionou sobre essa questão da legislação.

Expliquei-lhe detalhadamente e fiz uma analogia com outro caso, imaginando que se, hoje, ele e toda sua família fossem ameaçados de morte, por meio de um e-mail anônimo, dizendo que os matariam daqui a 10 dias. Amanhã, V. Exa. notificaria o provedor para ver quem seria o possível assassino; o provedor responde que precisa de uma ordem judicial; V. Exa. entra com um pedido de ordem judicial, que é atendido após dez dias; o provedor comunica que mantém arquivados os dados apenas por cinco dias. Cuidado, pois daqui a dez dias poderia acontecer alguma coisa.

Voltando ao caso anterior, depois de um tempo, a sentença converteu a obrigação não cumprida em perdas e danos, no valor, por danos materiais, em R$29.000,00 (vinte e nove mil reais) e também nos danos morais, dez vezes o valor dos danos materiais, R$290.000,00 (duzentos e noventa mil reais). Considero fantástica a decisão porque, enquanto não existir uma legislação específica, somente por meio de decisões judiciais como essa é possível balizar um regramento sobre este assunto. Tenho certeza de que se houver um novo caso, e esse provedor receber uma notificação extrajudicial de quem quer que seja, ele irá preocupar-se em preservar as informações.

Obviamente que existe recurso, está pendente de julgamento e pode ser reformada, principalmente a questão dos danos morais. Mas, trata-se de uma sentença bastante interessante sobre esse tipo de conduta.

Na prática, em relação a provedores de acesso, eles não devem responder direta e solidariamente pelo seu cliente, o autor do ilícito. Existem várias analogias. Seria o mesmo caso de responsabilizar a companhia telefônica por uma ligação anônima que se faz e que causa algum dano. Ela é responsável somente pela identificação e não pela preservação dos dados. Qual seria o meu conselho para os provedores de acesso? Cumprirem a recomendação de três anos pela preservação desses dados. Na prática, os casos da não preservação de dados são exceções;

na maioria das vezes, os provedores preservam os dados e os fornecem. Isso está tranquilo, atualmente. A legislação iria regulamentar esse assunto que é bastante coerente, porém é um caso interessante que compõe uma jurisprudência bem delimitada sobre esse assunto.

Falaremos sobre a responsabilidade dos bancos no caso de fraude na internet. Se um de nós observarmos na nossa conta uma transação que não reconhecemos, os senhores acreditam que o banco deve ser responsabilizado por isso? Sim, não ou depende? Sempre gosto mais do "depende". O banco não pode ressarcir diretamente a vítima nesse caso, porque seria muito simples. Por exemplo, um criminoso combinaria com um amigo, que tem uma conta bancária, que fará uma transferência para essa conta e ligará para o banco dizendo que não foi ele para depois dividirem o valor entre os dois. Por isso o banco não ressarciria, inclusive pela possibilidade da autofraude.

Os bancos respondem objetivamente, neste caso, pelo Código de Defesa do Consumidor. Porém, existem as exceções às responsabilidades objetivas. Simplificando, a grande exceção da responsabilidade objetiva é quando há culpa exclusiva da vítima.

Em termos práticos, citarei um caso em que houve uma fraude em uma empresa. Atualmente, a maioria dos bancos - isso depende do valor da fraude, para ver se comercialmente é bom ou não para o banco - normalmente pedem autorização para investigar, inclusive formalmente, o que aconteceu. A vítima ligou para o banco e avisa que sofreu uma fraude, este alega que se houve uma fraude via *internet banking*, provavelmente, o computador foi invadido e questiona se poderia analisar o computador para saber o que acontecera. Nesse caso, a vítima autorizou essa análise. Ao verificar o que havia ocorrido, o banco percebeu que na tela do computador tinha um *post it*, com *login* e senha de acesso ao *internet banking* da vítima. Ao analisar o HD do computador da vítima, percebeu que não tinha um antivírus há pelo menos seis anos.

Nesse aparelho, na verdade, não tinha um cavalo de Tróia, mas um "haras" de Tróia, ou seja, mais de cem códigos maliciosos.

Pergunto aos senhores: neste caso, deveria haver o ressarcimento ou seria culpa exclusiva da vítima? Afinal de contas, existe o contrato com o *internet banking*, que possui cláusulas específicas sobre a responsabilidade do usuário com as senhas, apesar de ser um contrato de adesão. Para o banco, o cliente é aquele *login* e aquela senha.

Neste caso, por um lado, o banco comprova que não houve nenhum tipo de negligência, imprudência ou imperícia de sua parte. De fato, neste tipo de situação, a fraude sempre está no usuário, porque, assim como no mundo real, o criminoso prefere roubar um carro com a porta aberta, com a chave no volante do que o outro que é blindado, que tem alarme e que tem *insulfilm*, pois é mais fácil. A parte mais frágil, nesses tipos de processo, são os usuários comuns. É praticamente impossível invadir o sistema de um banco, pois existem diversas normativas nacionais e internacionais, principalmente do Banco Central, sobre segurança dos seus sistemas. Se essa segurança for invadida, obviamente que nem se discute; se o banco já responde objetivamente, quanto mais no que diz respeito à responsabilidade subjetiva.

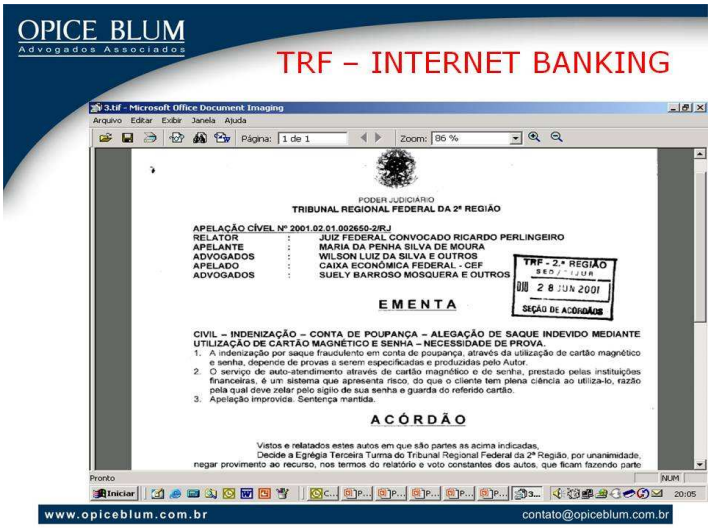
Neste caso, a corda mais fraca está do lado da vítima, pois a fraude foi cometida no seu computador.

A grande questão é saber qual o limite do senso comum de responsabilidade sobre os computadores. Será que, se não existir um antivírus atualizado, isso já caracteriza uma culpa exclusiva da vítima, ou será que precisa ter um *post it* na tela do computador, com *login* e senha? Ou precisa ter cinquenta e três códigos maliciosos no computador da vítima? Precisamos analisar qual é o limite da culpa exclusiva da vítima.

Temos outro exemplo, de um cliente que não reconheceu a transferência bancária em que foi confirmado que o filho da dona de uma empresa tinha colocado um *software* malicioso no computador da própria

mãe, que gravava as telas de acesso ao internet *banking*. A mãe não tinha conhecimento, processou o banco por causa daquela fraude. Enfim, esse filho está sendo processado por estelionato, porque ficou comprovado, nos computadores, que ele instalara aquele código malicioso para aplicar a fraude. A prova foi produzida na Vara Cível e encaminhada para inquérito policial. Atualmente, está em processo de investigação.

Existem algumas decisões judiciais que já demonstram uma tendência de se aplicar cada vez mais a questão do senso comum, do homem médio, para um conhecimento maior.



Para que os senhores possam ter uma idéia, citarei o exemplo de uma das decisões existentes, envolvendo cartão magnético e senha, do Tribunal Regional Federal da 2ª Região:

> A indenização por saque fraudulento em conta de poupança, através da utilização de cartão magnético e senha, depende de provas a serem especificadas e produzidas pelo autor, e não pelo réu. O serviço de autoatendimento de cartão magnético e de senha, prestado pelas instituições financeiras, é um sistema que apresenta risco, de que o cliente tem plena ciência ao utilizá-lo. Razão pela qual deve zelar pelo sigilo de sua senha e guarda do referido cartão.

Citando outro exemplo de fraude – antes do internet *banking*, tínhamos o acesso ao extrato bancário e até fazíamos transações por telefone, assim como fazemos, eventualmente, atualmente – tivemos um caso em que um fraudador ligou para um cliente de um banco, confirmou o seu nome, perguntou se ele tinha conta no banco, apresentou-se como funcionário da instituição e solicitou o seu *login* e senha, para fazer atualização do cadastro. O cliente passou-lhe as informações por telefone. Tivemos a seguinte decisão do Tribunal de Justiça do Distrito Federal:

Age com culpa o cliente que, sem tomar as devidas cautelas, fornece sua senha por telefone a pessoa que se apresenta como funcionário de estabelecimento bancário ao pretexto de que esta declinará alguns de seus dados pessoais, tais quais: CPF, número da conta e código de agência.

Nesse caso, o Tribunal decidiu pela culpa concorrente, pois extrapolou o limite permitido. Obviamente, o banco arca com o que passou desse limite. Vejam que há o reconhecimento. Qual a diferença deste caso, em que o sujeito passou os dados por telefone, para aquele caso virtual em que consta a mensagem: "você está sendo traído, clique aqui", e, com isso, instala-se um código malicioso? Podemos considerar a mesma situação, porém com tecnologias atuais diferentes.

Quanto à culpa exclusiva da vítima e à questão do Código de Defesa do Consumidor, existe a excludente, em que o fornecedor de serviço só não será responsabilizado quando comprovar a culpa exclusiva de terceiros. Não é interessante para os bancos discutir esse tipo de responsabilidade, porque isso não é bom para o marketing, para o nome do banco. O interessante é que cada vez mais essas discussões encerrem-se.

Se antes tínhamos apenas o *login* e senha para acesso ao *internet banking*, atualmente, cada vez mais, os bancos empregam novas tecnologias para os clientes, como por exemplo, a utilização do cartão de segurança. Na figura de um cartão de segurança, existe uma pequena cartela com quarenta senhas.

É o chamado "*token* de pobre". Quando alguém vai acessar o banco, existem quarenta senhas e deve-se clicar uma delas. Vejam: para fazermos uma transação via *internet banking* é preciso um dispositivo físico, como esse cartão. É necessário que se digite uma das senhas ofertadas pelo sistema. Juntamente com o cartão, vem a explicação de como utilizá-lo. Atenção: o banco solicita apenas uma senha por vez, mas existem os códigos maliciosos que pedem para o cliente digitar as quarenta senhas, e algumas pessoas o fazem, ficam durante muito tempo digitando-as.

Tudo isso tem que ser levado em conta caso a caso. Minha mãe, por exemplo, envia-me um e-mail por semana, perguntando se uma determinada mensagem é ou não um código malicioso. Antigamente, aprendia-se com o erro, mas, atualmente, depende da pessoa. O Juiz saberá analisar, quando se tratar de um senhor de idade que não tem condições de ter conhecimento, para ponderar o caso.

Mas, por bem ou por mal, recebe-se um contrato com esse cartão de segurança, em que está escrito que o banco solicita apenas uma senha por vez, e o código malicioso solicita as quarenta senhas. Mesmo assim, acontece de a pessoa digitar as quarenta senhas e depois processar o

banco. Este caso aproxima-se um pouco mais da culpa exclusiva da vítima.

Além do cartão de segurança, existe o *token,* que, a cada vez, oferece um número diferente, ou seja, é um número randômico. Cada vez que acessamos o banco, apertamos o botão do *token*, e aparece um número, por meio do qual permite-se o acesso. Então, não são mais quarenta senhas, são infinitas senhas aleatórias que vão mudando a cada vez, ou seja, é impossível haver um fraudador; não é possível cometer uma fraude.

Temos um exemplo de uma empresa em que o seu proprietário recebeu esse *token* para fazer transação, como representante legal da empresa, e o repassou para o seu "braço direito" na empresa, autorizando que ele fizesse as transações bancárias. Durante mais de um ano, mais de um milhão de fraudes foram desviadas da empresa. O dono da empresa descobriu e instaurou inquérito policial contra o seu "braço direito". O sujeito foi preso e, agora, o dono da empresa está processando o banco, alegando que este forneceu um *token,* colocou entre aspas na petição inicial, alegando que desconhecia aquele tipo de ferramenta, que não sabia que poderia emprestar a um terceiro e que a responsabilidade, neste caso, é totalmente do banco.

É difícil, dependendo do tipo de situação, fazer essa defesa. Obviamente, precisa ser solicitada a prova pericial para demonstrar que todas as transações foram legítimas e, neste caso, inclusive a prova contábil, pois como que, durante mais de um ano, mais de um milhão é desviado e não consta na Declaração do Imposto de Renda? Podemos deduzir que tem algo errado.

Por isso que, além do *token*, também existe a assinatura digital, que caso não seja a própria pessoa a utilizar, a Medida Provisória nº 2.200, de 2001, que tem força de lei, traz a responsabilidade do usuário. Então, se a pessoa emprestar para o contador ou deixar com alguém para alguma finalidade e esse alguém cometer algum tipo de conduta ilícita, a

responsabilidade, pela legislação, é diretamente desse usuário que concedeu a assinatura digital.

Temos outra decisão do Tribunal de Justiça do Rio Grande do Sul: "Quem navega na web deve, necessariamente, utilizar um programa antivírus." Vejam só como as decisões judiciais estão ficando modernas! Neste caso, a pessoa utilizava a internet e foi instalado um código malicioso, através de um dos *sites* pornográficos que ele acessou, – porque nada na internet é de graça, não existe isso, se tem alguma coisa gratuita desconfiem – que fazia ligações internacionais. Após um mês, constou na fatura da conta telefônica dessa pessoa um valor de cento e vinte reais relacionados a uma ligação internacional feita através do seu computador. Resultado: a pessoa não reconheceu aquela despesa e processou a empresa telefônica, alegando que não era responsável por aquela dívida, pedindo, inclusive, para retirar o seu nome dos órgãos de proteção ao crédito. Foi feita a instrução probatória, e ficou demonstrado que não foi instalado um antivírus na máquina. Veio essa decisão judicial que, basicamente, decide que houve culpa exclusiva da vítima, porque ela não tinha um antivírus. Obviamente, é difícil afirmar que existe a culpa exclusiva, porque não tinha o antivírus. É até um pouco arriscado uma decisão como essa, porque não significa que se tiver o antivírus estará salvo de tudo, mas mostra mais uma vez essa tendência em relação à proteção dos sistemas.

Temos mais um caso que mostra a importância do consumidor verificar, cuidadosamente, o *site* que acessa referente a e-*commerce* como um todo. Sabemos que um contrato não exige uma forma especial, então o que vale é a **pacta sunt servanda**, isto é, a vontade entre as partes. Não importa qual o meio ou formato que o contrato é realizado, ou seja, na maioria das vezes, quando compramos algo eletronicamente, em qualquer tipo de *site*, o aceite é feito pelo clique, o que significa a validação plena da manifestação da vontade.

Na grande maioria dos *sites*, existe uma política, não só de segurança da informação, mas muitas vezes de privacidade, que demonstram todas as cautelas que o consumidor deve ter em relação às pessoas que, eventualmente, estão vendendo os produtos no *site*. Existem até critérios de quem é o melhor vendedor, comprador e outros comentários. Neste caso, especificamente, o consumidor, apesar de ter assinado essa política, não a seguiu e depois processou o provedor, mas no final perdeu a ação.

Vejam o exemplo acima apresentado: Código de Defesa do Consumidor; compra na internet; fraude; não entrega do bem; serviço de aproximação comercial (compradores e vendedores); não utilização de ferramentas de controle disponibilizadas; inobservância à política de segurança; inobservância de regra de segurança constante na política do *site* de vendas; o CDC não pode ser invocado como anteparo paternalístico a respaldar condutas negligentes e de manifesto despreparo do consumidor no trato de seu patrimônio. Ou seja, se existe a política e está tudo esclarecido, por que aquela política não foi seguida?

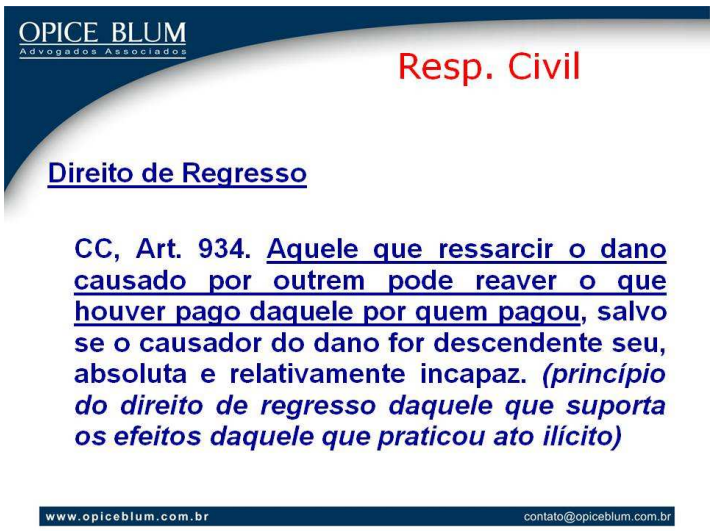
Estou trazendo vários exemplos contrários ao que, normalmente, observamos, obviamente, vai repetindo, vai depender muito de caso a caso, e, principalmente, da pessoa e das provas. É somente uma tendência das nossas decisões judiciais.

Vejamos alguns artigos: Art. 186. responsabilidade subjetiva; Art. 927. obrigação de reparação por ato ilícito; Parágrafo único. questão do risco da atividade.

Art. 944. A indenização mede-se pela extensão do dano; Art. 945. Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com o autor do dano. Culpa concorrente, o que pode ser muitas vezes balizada em relação a isso.

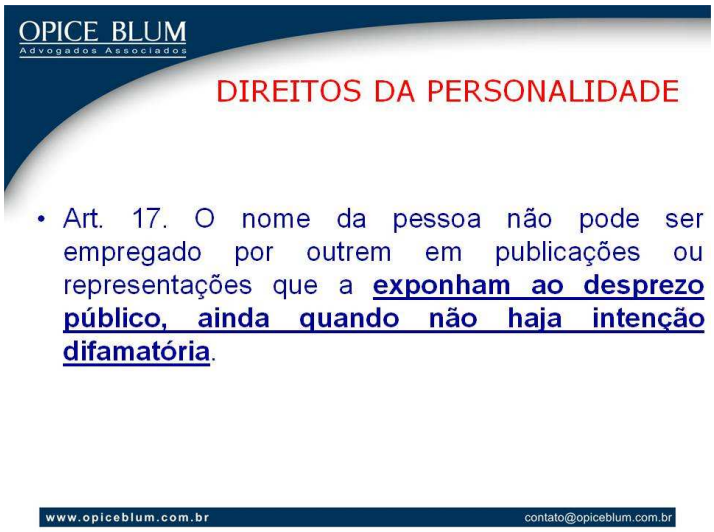
Responsabilidade Civil. Art. 932, inciso I e III. O inciso I trata da responsabilidade dos pais sobre os filhos e o inciso III

trata da responsabilidade do empregador pelos atos dos seus empregados, que justifica toda aquela questão do monitoramento.



Obviamente que naqueles casos do art. 932, inciso III, caso a empresa faça o ressarcimento pela responsabilidade solidária prevista, ela tem o direito de regresso, depois, contra o verdadeiro autor do ilícito, que é o art. 934 do Código Civil.

Direitos da personalidade. Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória. Lembramos todas aquelas situações relacionadas às situações vexatórias.



Estou mencionando inúmeros casos de gravidade relevante que, justamente e invariavelmente, envolvem uma questão que seria mais de privacidade, expondo-se ao mundo todo, porque é o que vem acontecendo, mas esses exemplos são os que ficam mais marcantes. São mais fáceis de serem ditos.

Contarei outro exemplo para todos, bastante grave. Um diretório acadêmico de uma universidade em São Paulo, assim como acontece todos os anos, realizou uma festa à fantasia. Nesta festa, tiveram a

brilhante idéia de fazer um cantinho do amor: pequenas cabines para os casais terem mais privacidade. Um indivíduo pegou uma câmera fotográfica digital e a levantava em cima do cantinho do amor para tirar fotos daqueles que estavam lá dentro. Posteriormente, este indivíduo, de posse de tais fotos, mandou-as para sete amigos, escrevendo em negrito e em caixa alta: "**PELO AMOR DE DEUS, NÃO PASSEM PARA NINGUÉM**", o que significa dizer: "Enviem para o mundo inteiro."

No dia seguinte, as fotos estavam na internet. Uma das principais vítimas teve que mudar do País, pois ela ainda estava estudando.

Neste caso concreto, tudo foi divulgado e, obviamente, ficou vinculado o nome da festa à universidade. Esta, além de ver o que aconteceu e constatar o autor do ilícito teve que desvincular aquele tipo de festa do nome da instituição como um todo. Foi possível verificar que uma das destinatárias da primeira mensagem que foi enviada com as fotos era aluna da instituição que contou haver recebido as fotos e propunha-se a abrir seu e-mail pessoal, autorizando a investigação.

No e-mail enviado utilizava-se o apelido de um dos alunos desta universidade, por isso foi identificado, através do IP e da quebra de sigilo, que a mensagem partiu, exatamente, do domicílio desse aluno. Verificou-se que ele estava cursando o último ano da universidade. Houve o procedimento administrativo com todo o contraditório e a ampla defesa, mas o aluno acabou sendo expulso da universidade. Por meio do Judiciário, ele tentou retornar ao seu curso, porém, não conseguiu.

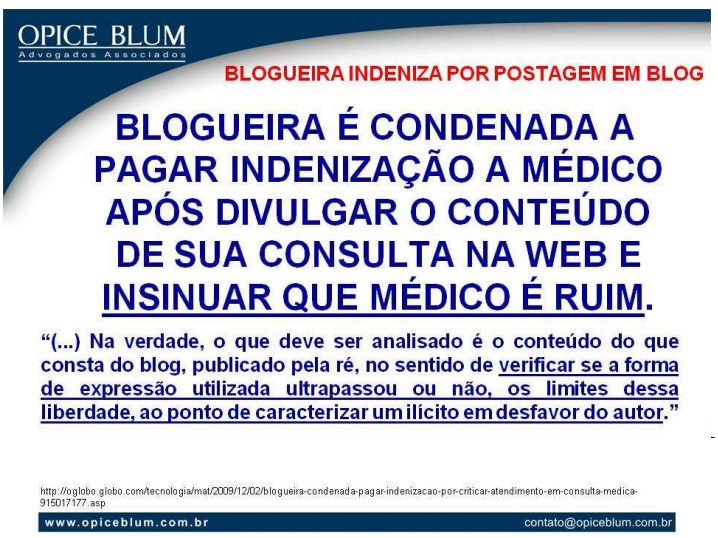
A principal vítima acabou processando, além do autor do ilícito e de diversos *sites* da internet, a própria instituição. Nas audiências, foram marcantes os depoimentos das vítimas que demonstram o potencial lesivo que tem a internet como um todo. Atualmente, essa aluna encontra-se matriculada em uma universidade no Brasil, após ter residido fora, mas, ainda assim, quando a lista de presença é passada, vinculam seu nome àquela festa, ou seja, até hoje este fato ficou marcado.

Salvo engano, a indenização, neste caso, contra o autor do ilícito, superou a quantia de quinhentos salários mínimos. Foram processados também, pela aluna, a universidade e o diretório acadêmico, tendo sido afastada a responsabilidade da universidade, que não tinha nenhuma ingerência sobre aquele tipo de evento, e o diretório acadêmico foi condenado a um valor menor por ter sido negligente e imprudente ao permitir este tipo de situação dentro de uma festa.

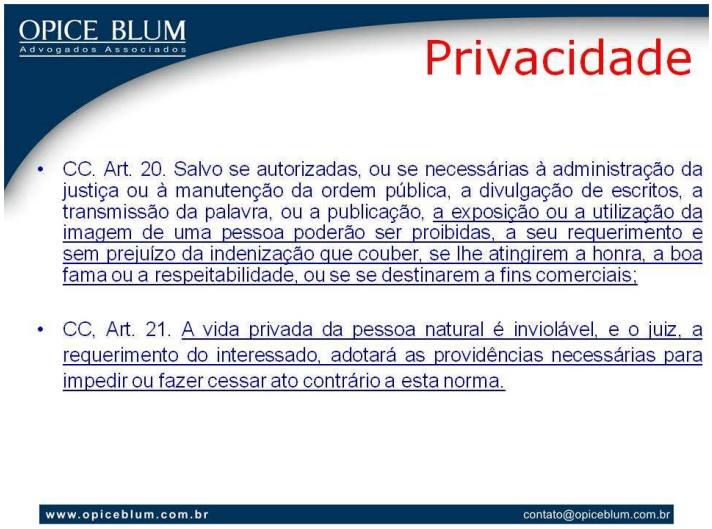
Enfim, trata-se de um caso bastante grave vinculado à questão do direito da personalidade.

Outro exemplo: a defesa do réu baseia-se essencialmente na tese de que apenas manifestou seu inconformismo com as decisões do órgão em que o autor trabalha. Porém, evidentemente, o réu não se limitou a criticar ou expressar inconformismo. Os textos falam por si e mostram que o réu atacou a honra da autora, atribuindo a ele a prática de crimes como fraudes e desvios de recursos. Conclui o magistrado: "É livre a crítica e o direito de expressão, mas cada um deve arcar com a responsabilidade dos seus atos, pois a Constituição também assegura o direito à honra, à intimidade e a privacidade". Trata-se daquele confronto entre liberdade de expressão e quando esta ultrapassa torna-se uma ofensa à honra e à dignidade da pessoa.

Blogueira indeniza por postagem em *blog*. Blogueira é condenada a pagar indenização a médico após divulgar o conteúdo de



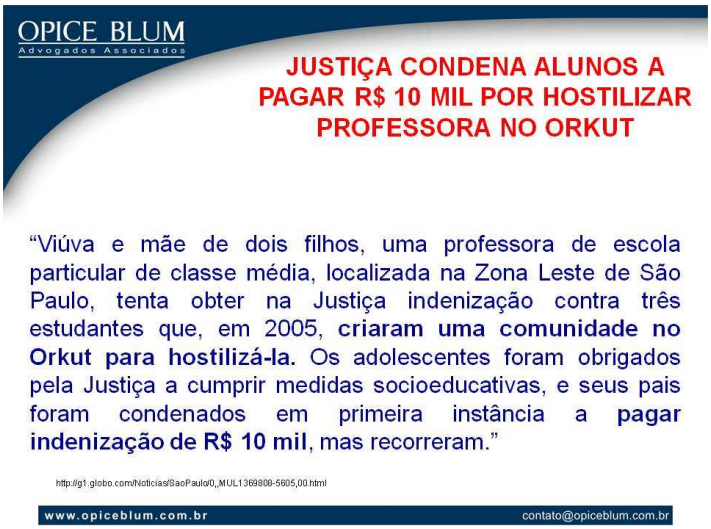
sua consulta na *web e* insinuar que o médico é ruim. "(...) Na verdade, o que deve ser analisado é o conteúdo do que consta no *blog* publicado pela ré, no sentido de verificar se a forma de expressão utilizada ultrapassou ou não os limites dessa liberdade, ao ponto de caracterizar o ilícito em desfavor do autor." Seria o velho direito da liberdade de expressão, que, se ultrapassados seus limites, poderá sofrer uma sanção.



Artigos 20 e 21 do Código Civil:

Art. 20. [...] a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

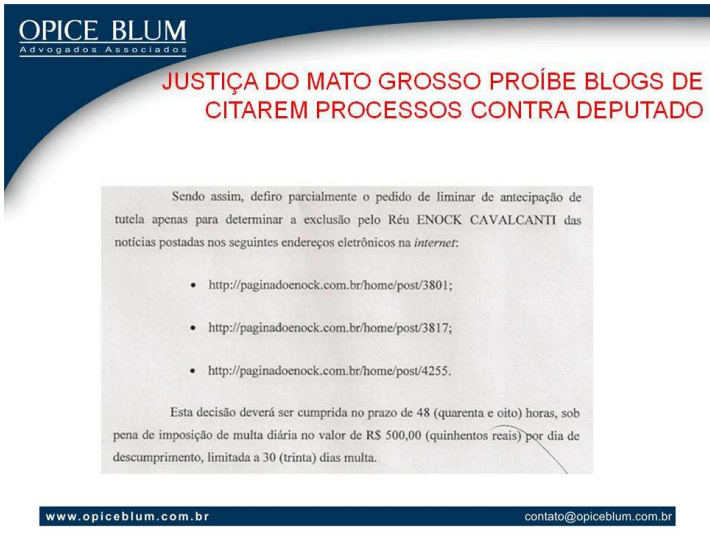


Cito outro exemplo:

"Viúva e mãe de dois filhos, uma professora de escola particular de classe média, em São Paulo, tenta obter na Justiça indenização contra três estudantes que, em 2005, criaram uma comunidade no Orkut para hostilizá-la. Os adolescentes foram obrigados pela Justiça a cumprir medidas socioeducativas, e seus pais foram condenados em primeira instância a pagar indenização de dez mil reais."

Este exemplo abrange o artigo 932, inciso I. Já existem casos julgados.

Justiça do Mato Grosso do Sul proíbe *blogs* de citarem processos contra deputado. Venho insistindo



nesta tese: não é em razão de termos a liberdade de expressão que, muitas vezes, se forem consideradas ofensivas, postagens não possam ser removidas, como ocorreu neste caso, em que a liminar foi deferida para tirar do ar esses *blogs* específicos.

Muitas vezes, há diversas consultas para saber da possibilidade da retirada de um nome da internet. Existem pessoas que desejam ficar totalmente ausentes da internet, pois, atualmente, se qualquer pessoa for pesquisada, pode aparecer algo a seu respeito.

Será que é possível solicitar uma ordem judicial para que o *Google*, ou outro buscador, remova todos os resultados de busca relacionados a uma determinada pessoa? O que os senhores pensam? É possível fazer um requerimento como este?

Têm que ser analisadas todas as postagens sobre a pessoa. Se houver postagens ilícitas, merecem ser removidas. Porém, não é possível retirar tudo da internet porque, muitas vezes, está dentro da liberdade de expressão, e, provavelmente, o juiz não irá aceitar o pedido. Como se fará uma vedação para o futuro, a fim de não permitir que digam algo sobre os senhores na internet dentro da liberdade de expressão?


OPICE BLUM
Advogados Associados

TJRS – Revista em Portal

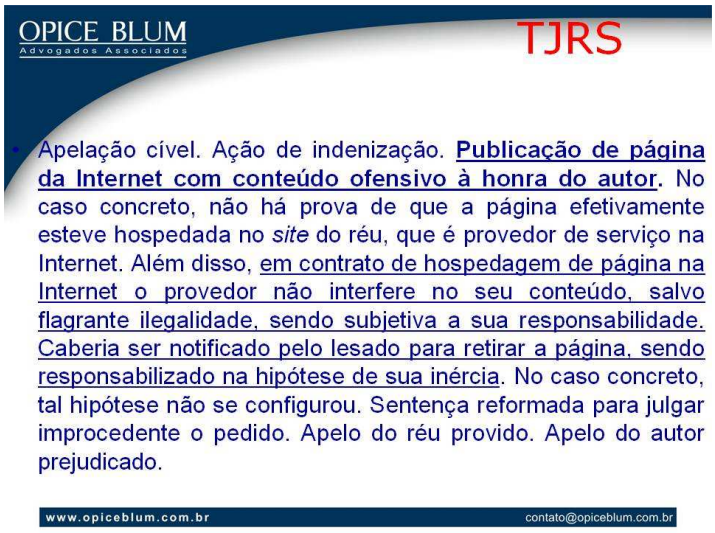
PROCESSUAL CIVIL. LEGITIMIDADE PASSIVA. PROVEDOR DE ACESSO E DE CONTEÚDO. INTERNET. DANO MORAL. RESPONSABILIDADE CIVIL. DENUNCIAÇÃO DA LIDE.
1 - É responsável o provedor de conteúdo da INTERNET (PSI) pela divulgação de matéria que viole direito e cause dano a outrem, seja por calúnia, difamação ou injúria, cabendo ao mesmo residir no pólo passivo da demanda onde a parte que se diz ofendida postula indenização por danos morais. Tal responsabilidade, contudo, não se reconhece ao provedor de conteúdo na hipótese em que este serve unicamente de meio de divulgação de revista, sendo esta perfeitamente identificável e responsável na forma da lei, por quaisquer manifestações de pensamento, ou mesmo de informação, que venham a causar violação de direito.

www.opiceblum.com.br contato@opiceblum.com.br

Revista em portal. Há algumas decisões judiciais sobre a responsabilidade dos provedores.

> "Tal responsabilidade, contudo, não se reconhece ao provedor de conteúdo na hipótese em que este serve unicamente de meio de divulgação de revista, sendo esta perfeitamente identificável e responsável na forma da lei, por quaisquer manifestações de pensamento, ou mesmo de informação, que venham a causar violação de direito.

Outra decisão:



Publicação de página na internet com conteúdo ofensivo à honra da autora.

[...] em contrato de hospedagem de página na internet o provedor não interfere no seu conteúdo, salvo flagrante ilegalidade, sendo subjetiva a sua responsabilidade. Caberia ser notificado pelo lesado para retirar a página, sendo responsabilizado na hipótese de sua inércia.

Este caso é bem interessante, porque, além da questão de mérito, existe a questão de provas que não constam desta parte. O sujeito alegava que, em uma página da internet – se não me engano, a cafajestes.com –, seu nome estava relacionado a algum tipo de conduta de cafajeste. Provavelmente, ele pressionou a tecla *print screen*, salvou a página no seu computador e imprimiu-a para juntar ao processo como prova da internet. Só que aquela página saiu do ar. Não se sabe, nos autos, se aquela página realmente existiu. O sujeito não preservou a prova adequadamente para instruir aquele tipo de processo.

Para preservarmos uma prova como essa, adequadamente, o ideal sempre é notificar o provedor, antes de pedir a remoção do ato ilícito, para que preserve seu conteúdo – ou seja, retira-se do ar, mas preserva-se o seu conteúdo – e fazer, também, o que é denominado, atualmente, de ata notarial, isto é, pedir para um cartório, com fé pública, imprimir aquela página, certificar e dar fé que acessou aquela página naquela data e naquele horário e que aquele conteúdo estava ali; se for discutida até essa ata notarial – pode ser discutida, porque o tabelião certificará fatos – o conteúdo estará preservado junto ao provedor. Então, pode ser feita uma prova pericial, e o provedor pode informar que aquela prova realmente existe.

O interessante, nessa decisão, é que o desembargador do Rio Grande do Sul, quando viu essa situação, até pesquisou na internet, em segunda instância, para ver se encontrava aquela menção na página virtual. Existe um *site* bem interessante, archive.org, que faz registros em *cache* de memórias antigas das páginas e os guarda. Por exemplo, se quisermos ver como era o portal Terra há seis anos, podemos encontrar algumas memórias em *cachê.* O desembargador descreve, no seu voto, que procurou no *site* archive.org e também não encontrou, por isso não considerou aquilo como prova, mas também pelo fato de a responsabilidade ser subjetiva, ou seja, não existir a prova. Ainda que existisse, o provedor falou que retira do ar tudo o que recebe em até quatro dias. Então, não caberia aqui uma indenização.

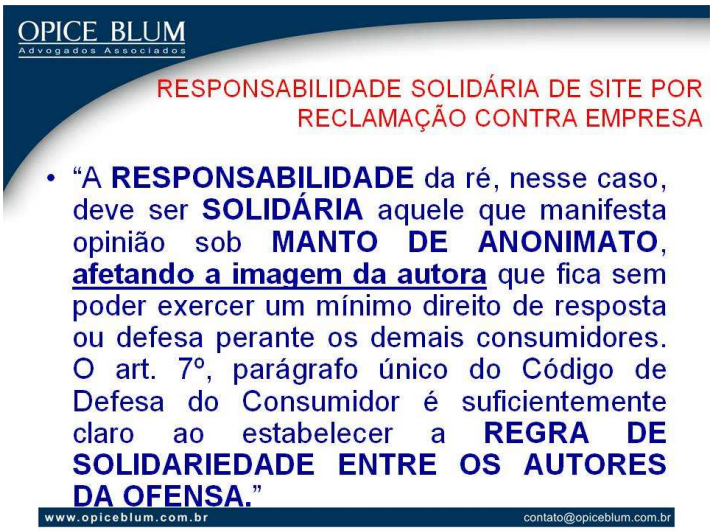
Existe um ponto interessante em que S. Exa. fala "salvo flagrante ilegalidade", ou seja, em caso de flagrante ilegalidade, o provedor responderia. O que seria flagrante ilegalidade neste caso? São os filtros que os provedores normalmente colocam. Quando envolvem casos de pornografia infantil, racismo e tráfico de entorpecentes, já existem certos filtros em que é possível fazer esse tipo de controle prévio, quer dizer, isso é retirado do ar previamente.

Para que os senhores tenham uma ideia da tecnologia em relação a esse tipo de situação, existem *softwares* que conseguem identificar fotos semelhantes uma das outras para também fazer uma verificação do que existe ou não na internet. Já se consegue vincular uma foto de um colega a outras fotos com rostos parecidos. Existem tecnologias no celular que, ao se apontar a câmera para o rosto de uma pessoa, se tiver essa base de dados, o celular dirá o nome completo dela.

Enfim, tudo é realidade, não é ficção. O interessante no Direito Eletrônico é que tudo deixa vestígio. Cada vez mais se tem como comprovar algo que antes seria praticamente impossível.

Outra decisão do Tribunal de Justiça do Estado de São Paul:

"criação de perfil falso de conteúdo gerador de responsabilidade civil do provedor, tão logo tome conhecimento de tal fato e persista no comportamento de mantê-lo."Responsabilidade subjetiva.



Outra decisão:

A responsabilidade da ré, nesse caso, deve ser solidária àquele que manifesta opinião sob manto do anonimato, afetando a imagem da autora.

Até agora, falamos de responsabilidade subjetiva de provedor de hospedagem, mas vejam como existem decisões que falam da responsabilidade objetiva, como seria neste caso:

> [...] manto do anonimato, afetando a imagem da autora que fica sem poder exercer um mínimo direito de resposta ou defesa perante os demais consumidores. O art. 7º, parágrafo único, do Código de Defesa do Consumidor é suficientemente claro ao estabelecer a regra de solidariedade entre os autores da ofensa.

Neste caso, tanto o provedor como o autor do ilícito seriam os responsáveis por isso.

Na minha opinião, o provedor de conteúdo apenas pode ser responsabilizado em duas hipóteses: na questão da responsabilidade subjetiva, se for notificado e não tirar do ar, ou se não tiver condições técnicas de identificar o responsável. Nessas duas hipóteses, ele poderia

responder. Quem precisa responder, em um primeiro momento, é o próprio autor do ilícito e não o provedor.

Outra decisão: indenização de R$ 30.000,00 (trinta mil reais):

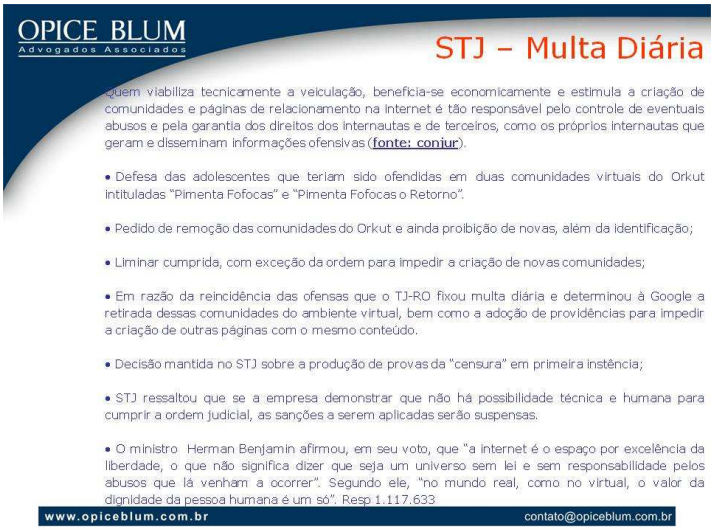
> Quanto à aplicabilidade do Código de Defesa do Consumidor, entende-se pela sua possibilidade. Embora a relação estabelecida entre as partes não possua remuneração direta, é notório que a remuneração se opera de forma indireta, na medida em que terceiros utilizam seus serviços para promover anúncios, tendo em vista o elevadíssimo número de acessos em seu *site*.
>
> A partir do momento em que a apelante não cria meios de identificação precisa do usuário, mas permite a criação de páginas pessoais em seu *site*, beneficiando-se, ainda que indiretamente, como dito acima, entende-se que ela assume o ônus pela má utilização dos serviços que disponibiliza, independentemente da existência de culpa.

O desembargador do Tribunal de Justiça do Rio de Janeiro está dizendo que para acessarmos esse tipo de comunidade, primeiro, é preciso identificar-se.

Sabemos, conforme já disse, que quando vamos abrir uma conta de e-mail não precisamos apresentar RG, CPF e comprovante de residência. Mas, por essa decisão, o desembargador diz que precisamos sim, porque consta a expressão: "não cria meios de identificação."

No meu entender, precisam ser guardados os registros eletrônicos do usuário, ou seja, número do IP (Protocolo de Internet), data e horário do acesso, o que já seria bem plausível, senão praticamente fica inviabilizado qualquer tipo de sistema eletrônico como esse *site* de relacionamento. Essa decisão é muito rígida ao reconhecer esse tipo de responsabilidade objetiva pelo risco do negócio.

Temos o exemplo de uma decisão do Superior Tribunal de Justiça, dessa semana, bem interessante também, falando da multa diária aplicada pela não remoção de uma página da internet. Vejam que interessante:



> Quem viabiliza tecnicamente a veiculação, beneficia-se economicamente e estimula a criação de comunidades e páginas de relacionamento na internet é tão responsável pelo controle de eventuais abusos e pela garantia dos direitos dos internautas e de terceiros, como os próprios internautas que geram e disseminam informações ofensivas.

Nesse caso, as adolescentes teriam sido ofendidas em duas comunidades intituladas "Pimenta Fofocas" e "Pimenta Fofocas, o Retorno". O requerimento pedia a remoção das comunidades e, ainda, publicação de novas, além da identificação.

A liminar foi cumprida, com a exceção da ordem para impedir a criação de novas comunidades, ou seja, houve o cumprimento para remoção daquelas, mas também houve a liminar para remover futuras comunidades.

Como se faz isso? É um controle posterior, que não é possível ter. O que ofende ou não? É subjetivo.

Em razão da reincidência das ofensas, o Tribunal de Justiça de Rondônia fixou multa diária e determinou à *Google* a retirada dessas comunidades do ambiente virtual, bem como a adoção de providências para impedir a criação de outras páginas com o mesmo conteúdo.

Decisão mantida no Superior Tribunal de Justiça sobre a produção de provas da censura em primeira instância.

O STJ ressaltou que, se a empresa demonstrar que não há possibilidade técnica e humana para cumprir a ordem judicial, as sanções a serem aplicadas serão suspensas.

O Sr. Ministro Herman Benjamin afirmou em seu voto que "a internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e sem responsabilidade pelos abusos que lá venham a ocorrer". Segundo Sua Excelência, "no mundo real, como no virtual, o valor da dignidade da pessoa humana é um só" – sem dúvida alguma.

Se os senhores analisarem tudo, a decisão do Superior Tribunal de Justiça (STJ) diz que a prova tem que ser produzida em primeira instância, sobre a viabilidade ou não de se censurar ou se remover tecnicamente páginas da internet. Não se está discutindo no STJ, propriamente dito, o mérito da questão, porque este será analisado na instrução probatória em primeira instância. É uma decisão marcante, porque não houve a remoção das comunidades futuras. O STJ está dizendo que, por enquanto, a liminar prevalece. Depois, se ficar caracterizada a inviabilidade técnica de se cumprir essa liminar, a multa não vai prevalecer, o que não é uma decisão de mérito também.

Outro caso bem interessante: "Justiça discute permanência de notícias na internet". O sujeito tinha sido condenado em primeira instância por um crime.

Posteriormente, não me lembro se foi absolvido ou se operou a decadência; enfim, ou extinguiu a punibilidade ou ele foi absolvido. Havia um portal na internet que tinha publicado a matéria quando ele foi condenado em primeira instância, só

que, atualmente, essa matéria está desatualizada. Porém, se alguém pesquisasse o nome dele em *sites* de busca, apareceria a matéria falando da condenação em primeira instância.

Como havia bastante acesso àquela matéria e, ao pesquisar o nome do sujeito, a primeira matéria que aparecia era, realmente, a matéria da condenação, o advogado solicitou que o juiz deferisse uma ordem judicial para que os *sites* de busca "randomizassem", ou seja, trocassem, aleatoriamente, os resultados das pesquisas para que não só aparecesse em primeiro lugar a pesquisa da condenação, mas outras matérias também sobre o sujeito. De fato, esse pedido foi deferido.

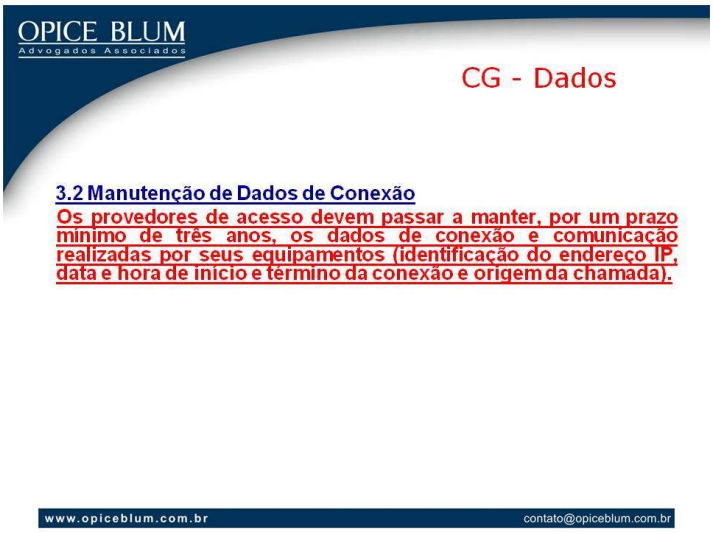
A questão é mais simples. Existem duas hipóteses: ou o provedor de conteúdo, que havia feito aquela matéria, atualiza, divulgando a absolvição, ou remove a matéria antiga do ar, que não está mais atualizada, e depois requer que os *sites* de busca façam uma atualização para que não encontrem mais, consequentemente, aquela matéria, uma vez que os *sites* de busca nada mais são do que robôs que estão buscando o que está no ar. Portanto, se a matéria não estiver mais no ar, será possível requerer para que não apareça mais aquele tipo de resultado.

Há outro caso bem legal. Conferência de dados de contrato eletrônico pela internet.

> Comete dano moral e o tem que reparar a empresa que aceita a contratação por meio eletrônico sem criar sistema de conferência de dados que lhes são fornecidos, preferindo correr os riscos que são de todos conhecidos.

Essa questão é mais ou menos simples, diz respeito ao mercado. Todos os *sites* de compra e venda não exigem, quando vamos fazer uma compra com cartão de crédito, uma certificação digital ou uma senha,

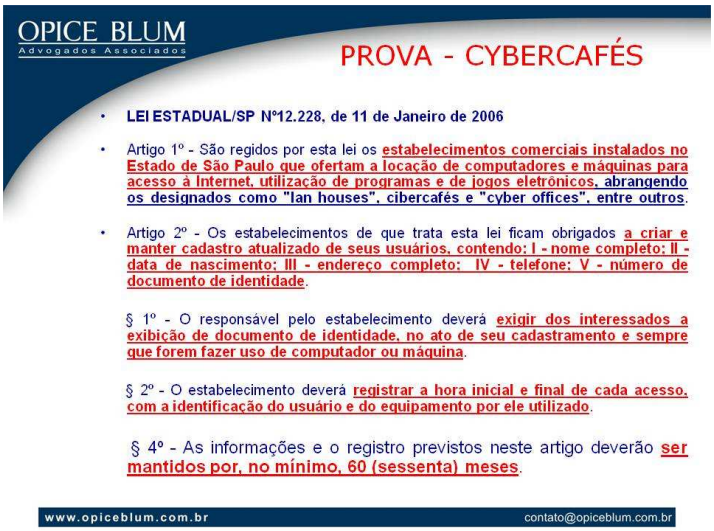
porque pouquíssimas pessoas no Brasil os têm. Por isso, preferem correr o risco de algumas fraudes e ser responsabilizados do que exigir esse tipo de informação, visto que, posteriormente, ele não conseguirá ter o lucro que teria.



Eis a recomendação em relação ao provedor de acesso, sobre a qual comentei com os senhores, que trata da responsabilidade do provedor de acesso, recomendação do Comitê Gestor da internet*:*

> Os provedores de acesso devem passar a manter, por um prazo mínimo de três anos, os dados de conexão e comunicação realizados por seus equipamentos, identificação de endereço, IP, data, hora de início e término da conexão e origem da chamada.

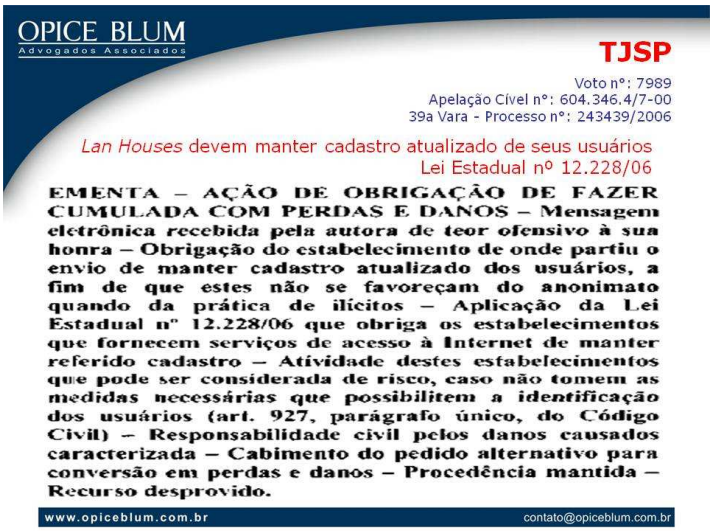
Isso deveria ser lei e não apenas uma recomendação.



Se o ilícito partir de uma l*an house,* como faremos para identificar? Qual a responsabilidade da *lan house* na identificação dos seus usuários? Em diversos Estados do Brasil, são leis estaduais e não federais. Existe uma legislação extremamente parecida com a do Estado de São Paulo, segundo a qual as *lan houses* devem guardar os dados dos seus clientes pelo prazo de sessenta meses, cinco anos; ou seja, identificação na hora da utilização do computador com data e hora de início e de término da conexão, justamente em razão de, se ocorrer algum ilícito ali dentro, ser possível a identificação.

Vejam que interessante. A Lei Estadual nº 12.228/2006, em seu art. 1º, diz que:

"São regidos por esta lei estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação dos computadores (...)". Repito, locação. Nem toda lei é perfeita, pois existem lugares em que podemos comer sanduíches e também utilizar a internet gratuitamente como comodato, o que não seria locação. Será que esses estabelecimentos estariam dentro dessa lei? Esse é um tipo de problema.


OPICE BLUM
Advogados Associados

TJSP

Voto nº: 7989
Apelação Cível nº: 604.346.4/7-00
39a Vara - Processo nº: 243439/2006

Lan Houses devem manter cadastro atualizado de seus usuários
Lei Estadual nº 12.228/06

EMENTA – AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM PERDAS E DANOS – Mensagem eletrônica recebida pela autora de teor ofensivo à sua honra – Obrigação do estabelecimento de onde partiu o envio de manter cadastro atualizado dos usuários, a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos – Aplicação da Lei Estadual nº 12.228/06 que obriga os estabelecimentos que fornecem serviços de acesso à Internet de manter referido cadastro – Atividade destes estabelecimentos que pode ser considerada de risco, caso não tomem as medidas necessárias que possibilitem a identificação dos usuários (art. 927, parágrafo único, do Código Civil) – Responsabilidade civil pelos danos causados caracterizada – Cabimento do pedido alternativo para conversão em perdas e danos – Procedência mantida – Recurso desprovido.

www.opiceblum.com.br contato@opiceblum.com.br

Vejam que interessante essa decisão judicial. Neste caso, que aconteceu em São Paulo, houve uma ofensa por meio de um *e-mail.* Foi identificado o provedor de acesso, que era a companhia telefônica; que identificou a origem, que identificou uma *lan house*.

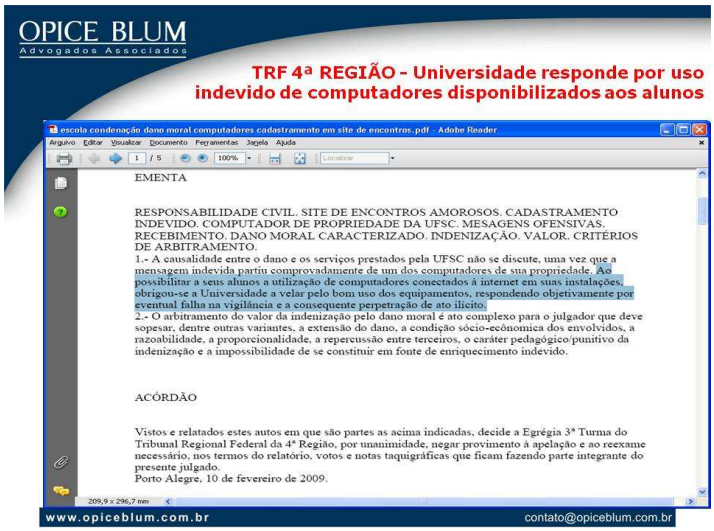
De acordo com a lei, pedimos que a *lan house* fosse oficiada para informar o dado do cliente responsável pelo ato ilícito. Nos autos do processo, a *lan house* respondeu que cumpria a lei estadual, pois identificava quem locava o acesso à internet, porém a *lan house* tinha também acesso por conexão sem fio, e quem a utilizava não deveria pagar a locação; ou seja, não tinha a identificação de quem foi o autor desse ilícito, porque, provavelmente, ele havia utilizado a conexão sem fio. Portanto, houve a impossibilidade de se identificar o autor do ilícito. Como resultado houve a conversão em perdas e danos contra a *lan house* no valor de R$ 10.000,00 (dez mil reais), decisão do Tribunal de Justiça do Estado de São Paulo, transitada em julgado.

Vejam que interessante:

> Mensagem eletrônica recebida pela autora de teor ofensivo à sua honra. Obrigação do estabelecimento de onde partiu o envio de manter cadastro atualizado dos usuários, a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos. Aplicação da Lei Estadual nº 12.228/2006, que obriga os estabelecimentos que forneçam serviços de acesso à internet de manter o referido cadastro. Atividade desses estabelecimentos que pode ser considerada de risco, caso não tomem as medidas necessárias que possibilitem a identificação dos usuários. Responsabilidade civil pelos danos causados caracterizada. Cabimento do pedido alternativo para conversão em perdas e danos. Procedência mantida.

Ou seja, não só pela lei, mas pelo risco da atividade aqui, a *lan house* foi condenada.

Essa lei deveria ser federal também, não só estadual, mas a tendência é que, cada vez mais, esse tipo de legislação tenha um trâmite mais rápido no Congresso Nacional.



Outro exemplo de um estudante que acessou a internet utilizando um computador dentro da universidade para praticar um ato ilícito. A universidade respondeu por ter provido o acesso e por não conseguir identificar o responsável.

Vejam que interessante mais este caso. Na Índia, donos de redes *Wi-Fi* desprotegidas podem ir para a prisão, por exemplo. Normalmente, aquele que provê comercialmente esse tipo de acesso tem que

identificar os autores do ilícito.

Quanto à pessoa física que instala uma rede *Wi-Fi* na sua residência, desprotegidamente, e de repente, alguém estaciona o carro na frente da sua casa e acessa a rede para praticar algum ilícito, o protocolo da internet vai recair na casa daquela pessoa, que não terá como identificar o responsável. Será que ela deve ser responsabilizada por isso? Converter em perdas e danos? Já temos uma noção suficiente de tecnologia para saber que, a partir do momento em que se instala uma rede W*i-Fi* em nossas residências, precisamos protegê-la?

A meu ver, as empresas que vendem estações, redes W*i-Fi*, de uma forma geral, deveriam ser obrigadas a vender esse tipo de equipamento ou de serviço bloqueado, ou seja, com senha. Se o usuário quiser, ele que acesse essa rede sem senha, e ele que passe a ser responsável por aquilo, mas não há nada definido nesse sentido.

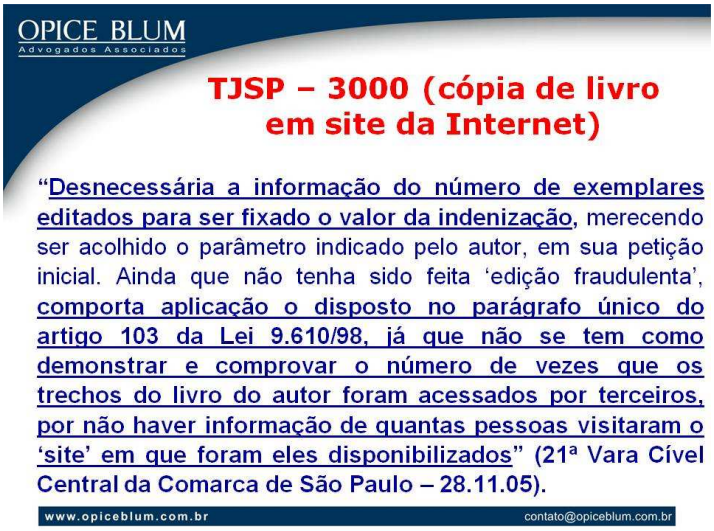
Como já disse anteriormente, provavelmente, começará a ser construído um marco regulatório civil, e, dentro deste, já fizemos nossas sugestões por meio do Conselho da Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (Fecomércio) de que, justamente, uma das hipóteses seja a de que, quando se tratar de redes sem fio, as empresas que prestam esses serviços ou vendam esses produtos passem a vender ou disponibilizar esses produtos por meio de uma conexão fechada; e,depois, sob responsabilidade do usuário, que eles possam acessar ou não, dependendo da situação.

Imaginem a situação em que um provedor de acesso, no momento de identificar o autor de um ilícito, equivocar-se e fornecer o dado de outra

pessoa, ou seja, inicia-se uma investigação por um equívoco do provedor de acesso contra uma pessoa que não tem nada a ver com o fato. Na maioria das vezes, quando falamos de pessoa física, o IP é dinâmico; ou seja, cada vez que acessamos a internet, recebemos um IP diferente. Então, precisa ser exatamente aquele IP, naquela data e naquele horário.

Neste caso, o provedor equivocou-se e atirou na loteria, ao indicar justamente um promotor de justiça. Felizmente, não houve uma busca e apreensão. Instaurou-se apenas um procedimento investigativo e, neste caso, o promotor de Justiça, em razão da falha do provedor de acesso, ganhou uma ação de indenização de R$ 60.000,00 (sessenta mil reais).

Falarei um pouco sobre direitos autorais. Podemos partir de uma premissa, segundo a Lei nº 9.610/98, que é a lei que regulamenta os direitos autorais, que provavelmente 60% a 70% de tudo o que está na internet é violação de direitos autorais, porque não tem qualquer tipo de proteção.



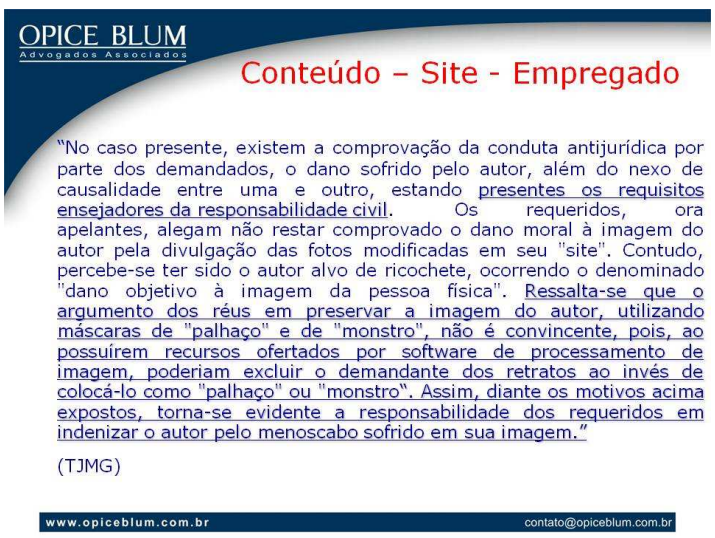
Neste exemplo, um médico de Rondônia transcreveu 80% do livro de um perito no seu *site*, sem qualquer informação sobre a fonte. Este processo é público; foi divulgado amplamente pelos meios eletrônicos quando saiu essa decisão. Mesmo que tivesse a informação sobre a fonte, a lei permite apenas transcrever pequenos trechos, e não 80% do livro. Se alguém acessasse a página daquele médico teria certeza absoluta de que aquele conteúdo era da sua autoria. Enfim, houve a violação aos direitos autorais.

Vamos deixar a parte criminal de lado, o art. 184 do Código Penal, e vamos analisar a responsabilidade civil. Vamos preservar a prova

adequadamente. Interpelação ao provedor de hospedagem para preservar a prova. Ata notarial, comprovando que aquilo realmente estava no ar.

Qual é o valor da indenização neste caso? Se alguém copiar um livro, o valor da indenização é o valor do livro. Como estava em um *site* da internet, qual seria o valor dessa indenização por danos materiais? Poderíamos verificar quantas vezes aquele *link* em que estava disponibilizado o livro foi acessado, mas quem tem essa informação é o contrafator ou provedor de hospedagem, que é contratado por ele, portanto estão juntos; ou seja, essa informação pode ser facilmente adulterada ou apagada. O art. 103 da Lei 9.610/98 menciona que quando não for possível contabilizar o número de edições fraudulentas, aplica-se três mil vezes o valor. Assim, ao imputar a responsabilidade do número de acessos para a parte contrária e não para o autor, estaremos requerendo três mil vezes o valor de 80% do livro, alegando que quem teria o número da quantidade de acessos seria a parte contrária e não o autor.

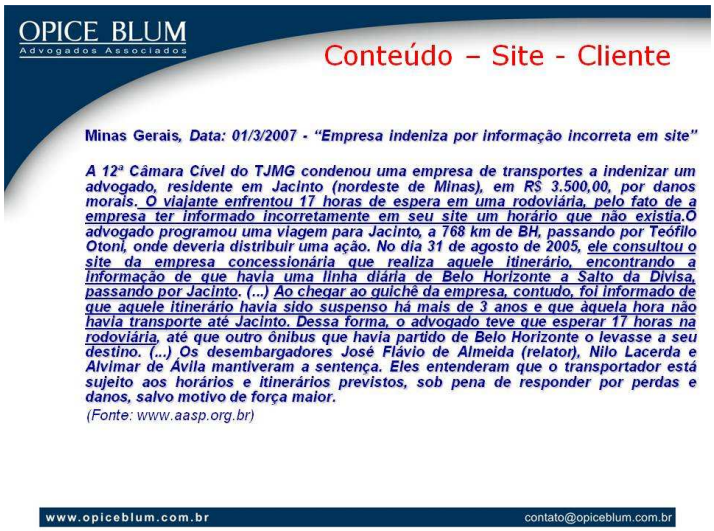
Na contestação da parte contrária, que tinha umas três folhas, dizia basicamente que o que está na internet é público e, portanto, não houve violação de direitos autorais, isto é, confessou que havia violado os direitos autorais, mas não rebateu a questão do valor da indenização. O resultado foi indenizar em três mil vezes o valor de 80% do livro. O advogado de defesa, nesse tipo de situação, deveria ter verificado quantos acessos tiveram. Se houvesse menos de três mil acessos, preservar-se-ia a prova eletrônica, adequadamente, para demonstrar. Nesse caso, a indenização iria variar de acordo com o número de acessos. Mas, como não houve essa contestação, manteve-se o valor de três mil vezes.



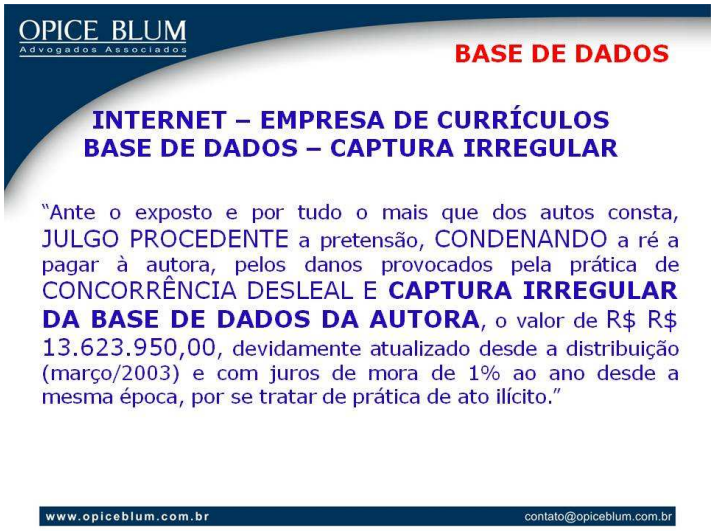
Prossigo com algumas outras decisões. Vejam só a criatividade! Às vezes, não acredito nesse tipo de conduta por parte de algumas empresas. A

empresa tinha um portal com a foto de todos os funcionários. O funcionário foi demitido e, na sequência, a empresa colocou na foto do funcionário, no Portal, uma máscara de palhaço e uma de monstro. Obviamente, o funcionário processou a empresa. Esta alegou que, pelo fato de o funcionário ter sido demitido, ele não poderia mais aparecer no portal, por isso colocaram uma máscara de palhaço e de monstro para ele não aparecer mais.

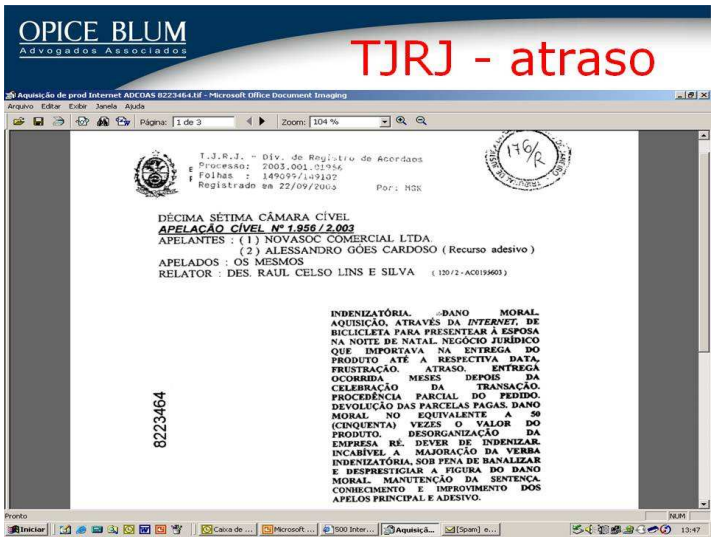
> Ressalta-se que o argumento das rés em preservar a imagem do autor, utilizando máscaras de palhaço e monstro, não é convincente, pois, ao possuírem recursos ofertados por *software* de processamento de imagem, poderiam excluir o demandante dos retratos, ao invés de colocá-lo como palhaço ou monstro. Assim, diante os motivos, torna-se evidente a responsabilidade em indenizar pelo menoscabo sofrido à sua imagem.



Dando continuidade, destaco a importância de as empresas manterem os seus *sites* atualizados. Neste caso, um advogado iria viajar de ônibus de uma cidade para outra. Antes de viajar, verificou o itinerário pela internet *e c*onstatou, exatamente, o horário que o ônibus iria sair da segunda cidade. Porém, esse *site* não estava atualizado há mais de três anos, por isso teve que ficar dezessete horas na rodoviária. Resultado: ele entrou com uma ação e ganhou R$ 3.500,00 (três mil e quinhentos reais) por danos morais. Então, sempre vale a recomendação de que, caso o *site* não esteja atualizado, principalmente os que envolvem esse tipo de serviço, deve deixar claro que é melhor entrar em contato por telefone para confirmar, porque, muitas vezes, pode haver uma alteração de horário.



Mais um exemplo: este caso é famoso em São Paulo, envolvendo a concorrência desleal de banco de dados de currículos, em que ficou comprovado que uma empresa concorrente tinha tido acesso à base de dados da outra e, por isso, houve a indenização em primeira instância, no valor de R$ 13.623.950,00 (treze milhões, seiscentos e vinte e três mil e novecentos e cinquenta reais



No que se refere ao caso de atraso na compra e venda através de portais via *internet*, lojas virtuais, neste caso, uma pessoa comprou uma bicicleta para presentear seu filho no Natal e a bicicleta só chegou um mês depois ou nem chegou. Como envolvia uma data especial e tinha um contrato eletrônico que previa a entrega do bem até aquela data, houve a responsabilidade, em razão desse não cumprimento do contrato.

Para finalizar, há uma decisão bem interessante, que vincula aqueles portais denominados *sites* de leilão na *internet*. Como disse, a responsabilidade é por

aproximar compradores e vendedores, e não uma responsabilidade direta. Acontece que, muitas vezes, consumidores mal intencionados localizam produtos que estão muito abaixo do valor que realmente custariam, adquirem aqueles produtos, sabem que não os receberão e processam o *site*.

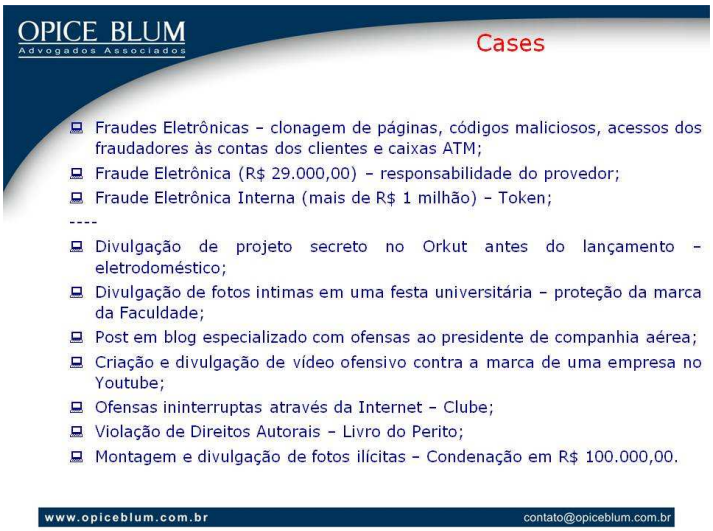
Neste caso, uma pessoa adquiriu dois computadores pelo valor de R$ 7.800,00 (sete mil e oitocentos reais), que deveria na época custar R$ 10.215,00 (dez mil, duzentos e quinze reais).

Disse o juiz:

> O autor sabia disso e, mesmo assim, tentou se dar bem ao adquirir não um, mas dois computadores no valor unitário de seis mil novecentos e noventa reais, e não se diga que ele é um consumidor e, por isso, a parte mais fraca, pois o documento de fls. tal dá conta de que ele é acostumado a comprar pela Internet, vinha pesquisando os preços. Ele sabia, sim, que o preço era mais barato e deveria, portanto, ser o produto fruto de contrabando ou roubo. Ele, portanto, aparentemente, tentava ser cúmplice de receptação ou sonegação fiscal. Tanto é assim que comprou numa empresa sediada no bairro de Santa Efigênia, notório paraíso de contrabando e pirataria e sede do império de Law Kim Chong, onde pessoas bem intencionadas não adquirem nada. Além do mais, pagou a uma pessoa física e não à empresa, o que demonstra triangulação para burlar o fisco. Ele não é nenhum idiota, pois é médico veterinário. É vítima de estelionato. Típico é nesse tipo de crime, a vítima ser um pretenso estelionatário que encontrou um esperto maior. É o padrão em todos os crimes do gênero.
>
> Indefiro a antecipação de tutela. Remetam-se cópia dos autos à Polícia Federal e à 1ª DP de Brasília, Secretaria de Segurança de São Paulo, Secretaria da Receita Federal, Secretaria da Fazenda de São Paulo, Secretaria da Fazenda do Distrito Federal, Secretaria da Fazenda do Município de São Paulo e à CPI da Pirataria.

Acredito que essa pessoa, mesmo se tiver algum direito na vida, nunca mais vai procurar o Judiciário, com medo. Mas, enfim, tirando alguns excessos da decisão judicial, ela é coerente em relação à questão da responsabilidade como um todo.

Temos alguns *cases* que trouxe para distribuir para os senhores em *slides*. Trata-se de casos que comentei com a citação de cada um.



O *slide* final que quero deixar para os senhores é este: "O computador disse que preciso fazer um *up grade* do meu cérebro para ficar compatível com esse novo *software".*

É impossível acompanhar a tecnologia e isso é um fato. Não adianta ficarmos falando em inclusão digital, sem falarmos em conscientização, educação e segurança como um todo. Não adianta prover acesso, gratuitamente, ou de uma forma barata, fornecer computadores baratos sem que haja uma educação digital.

Assim como a questão da legislação. É impossível a legislação acompanhar as novas tecnologias. O bom disso tudo é que, atualmente, a maioria dos casos que acontecem e, hoje, pude passar um pouquinho dessa experiência que tenho para os senhores, já existe uma legislação pertinente. Sempre esperamos, diante disso tudo, que o Poder Judiciário, como um todo, consiga realmente acompanhar esses novos casos e saiba aplicar o Direito, principalmente em razão de ser uma ciência humana e

subjetiva, em relação ao potencial lesivo que traz todas essas novas tecnologias.

Precisamos aprimorar alguns pequenos pontos dessa legislação, mas o positivo disso tudo é que a grande parte já está prevista. Já são mais de dezessete mil decisões judiciais sobre o assunto, ou seja, isso é a mais pura realidade. No Brasil, a expectativa é que daqui a cinco ou dez anos, 90% dos crimes se dêem através dos meios eletrônicos. Então, não há mais como fugir dessa matéria. Um exemplo disso foi a primeira palestra sobre o Processo Eletrônico. Os advogados e o Poder Judiciário, como um todo, vão ter que estar acostumados com as novas tecnologias.

Deixo aqui exemplos de algumas cartilhas bem interessantes, que podem ser acessadas nesses portais. Há uma cartilha feita pela Fecomércio sobre o monitoramento eletrônico nas empresas; tem o grupo do Infosec, feito pela *Microsoft,* que envolve todas essas discussões sobre a segurança da informação; outra cartilha da Fecomércio sobre os perigos da internet; tem um guia do Serasa (Centralização dos Serviços Bancários S/A) com orientação sobre a questão de vírus, *hackers* e outras ameaças; e, tem outra cartilha falando sobre como navegar de forma segura.

Estamos com outro projeto na OAB/SP e, provavelmente, ainda este ano será lançada uma cartilha sobre segurança da informação dentro de casa. Haverá grande divulgação. Espero disseminar não só para o STJ, mas para toda a comunidade jurídica e as demais entidades.

Deixo a sugestão do livro: “Manual do Direito Eletrônico”, que foi comentado na primeira palestra. Se quiserem, fiquem à vontade para se cadastrar no *mailing* do escritório.

Falando um pouquinho sobre *spam,* isso não é *spam* de forma alguma, porque a questão do *spam* envolve *opt in* e *opt out*, ou seja, requerer o recebimento daquela mensagem e também a possibilidade de não mais recebê-las. Essa é a boa prática do *e-mail marketing* de uma forma geral, inclusive, prevista por um código de autorregulamentação. As boas práticas, apesar de não haver lei específica sobre o assunto, sugerem *opt in* e *opt out*. Também há o *software opt in*, aquele relacionamento prévio, ou seja, se encontrei alguém em uma palestra, teria o *software opt in* e o software *opt out*. Se os senhores quiserem receber notícias, decisões ou matérias sobre esse assunto fiquem à vontade no cadastramento no *site* do escritório.

Agora, sim, agradeço definitivamente a presença de todos!

Mais uma vez, agradeço ao Instituto dos Magistrados do Distrito Federal e ao STJ pelo convite. Tive muito prazer, uma grande satisfação e uma grande honra estar aqui.

Obrigado por tudo e um grande abraço!

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Iniciaremos a segunda e última palestra desta tarde, com o tema *Questões Tributárias do Direito Eletrônico*. Para ministrá-la, convidamos o palestrante Dr. André Alves Portella.

O Dr. André Alves Portela é Mestre e Doutor em Direito Financeiro e Tributário, pela *Universidad Complutense de Madrid* e Professor Adjunto dos Cursos de Mestrado e Graduação em Direito da Universidade Católica de Salvador; é ainda Pesquisador e Consultor do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ) e da Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e é Coordenador do Núcleo de Estudos em Tributação e Finanças Públicas (NEF), a quem passo a palavra.

PALESTRA IV: QUESTÕES TRIBUTÁRIAS DO DIREITO ELETRÔNICO

ANDRÉ ALVES PORTELLA
Doutor e Mestre em Direito Financeiro e Tributário – Universidad Complutense de Madrid

Boa tarde a todos.

Gostaria, inicialmente, de agradecer ao convite que me foi feito pela organização do evento, sobretudo na pessoa do Presidente, que se encontra presente, assim como à pessoa que fez o contato, que parece não estar presente, mas teria grande prazer em conhecê-la, a Sra. Carolina Plentz, da Área Executiva da coordenação do evento; portanto, fica registrado o agradecimento pelo tratamento extremamente atencioso que me foi dispensado.

Tenho doutorado em Direito, fiz alguns cursos na Europa, na Inglaterra, na Espanha e em Portugal e o tema da minha tese, não por coincidência a minha presença neste evento, foi exatamente quanto à questão da tributação do comércio eletrônico, mais especificamente do controle tributário do comércio eletrônico, tema da minha monografia, publicada em 2008, pela Editora Fórum. Para aqueles que tenham interesse no aprofundamento dessa matéria, seria uma leitura que indicaria, porque trata bastante do que será abordado no dia de hoje.

Atualmente, sou Advogado em Salvador e advogo muito com prefeituras. Tenho uma empresa de consultoria que, por incrível que pareça, realiza exatamente trabalhos no sentido da modernização das fazendas públicas municipais e estaduais, trabalhamos na área principalmente da inclusão digital das prefeituras, mais especificamente da Bahia, além de outros estados do Nordeste, com firma eletrônica, com certidão negativa eletrônica e com a nota fiscal telemática. Faço tais observações porque é, exatamente, a área de atuação do nosso grupo de, mais ou menos, vinte pessoas que lidero no Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ).

Em relação ao tema da tributação sobre o comércio eletrônico, temos discutido muito Brasil afora, viajando e falando em várias ocasiões e em fóruns como este, o que é interessante, obviamente, porque são várias as questões em que poderíamos levantar os diversos problemas e adequações necessárias em termos de tributação do comércio eletrônico, mas, para sistematizar o que venham a ser essas questões, proporia, neste caso, a divisão de todas essas implicações em três grandes grupos.

Então, qual o impacto que a internet ou as novas tecnologias da informação provocam – e aqui me permito usar como sinônimo o termo internet ao tratar das novas tecnologias da informação – em relação ao Direito Tributário?

É verdade que grande parte das observações que faremos ao longo desta palestra e do exame de todas as implicações que a internet tem sobre o Direito tributário, perceberão que, em muitos casos, tudo aquilo que falaremos aplicar-se-á também a outros ramos do Direito, ao Direito Civil, ao Direito Eleitoral e ao Direito Administrativo.

Quais seriam esses três grandes grupos? Diria, em primeiro lugar, o das implicações que a internet traz para o Direito Tributário material. Existem algumas observações a serem feitas e vamos tratá-las neste encontro.

Existe outro grupo relativo às implicações que tem a internet e as novas tecnologias da informação sobre o Direito Tributário formal, relativo, portanto, aos procedimentos, sobretudo de gestão e de controle do comércio eletrônico para efeito de tributação; e, em terceiro lugar, diria que existe também um terceiro grande grupo de implicações relativo ao controle das operações comerciais que se realizam por meio da internet, em outras palavras, o próprio controle tributário do comércio eletrônico.

Existiriam esses três grandes grupos muito bem definidos: implicações no Direito Tributário material, implicações sobre o Direito

Tributário formal e, por fim, as implicações que a internet terá no que diz respeito à incidência tributária sobre as operações comerciais levadas a cabo por meio da internet.

Em relação ao primeiro grupo de questões, as implicações do Direito Tributário material ou da internet sobre o Direito Tributário material, subdividiria as muitas implicações em dois grandes grupos por sua vez. Dentro do Direito Tributário material, observaremos primeiro algumas modificações ou consequências no que diz respeito ao plano normativo e, em segundo lugar, implicações no que dizem respeito a institutos e conceitos de Direito Tributário. Assim, dentro do Direito material, a primeira discussão é relativa, portanto, ao plano normativo. O que temos de implicação? O que a internet traz para o Direito Tributário material no que diz respeito ao plano normativo?

Nesse caso, a discussão é saber se existe a necessidade de se ter um sistema tributário específico para o tratamento das operações relativas ao comércio eletrônico. É necessário erigirmos um sistema tributário, um ordenamento jurídico tributário específico para esse tipo de operação, que caminharia em paralelo àquele Direito Tributário material, que é aplicável às operações no âmbito do comércio tradicional, e, nesse caso, há também três grandes correntes doutrinárias.

Existe uma primeira corrente que defende que não é, em absoluto, necessário se ter a construção de um Direito Tributário, de um âmbito normativo específico para o tratamento das operações de comércio eletrônico.

Nesse caso, temos como grandes representantes dessa linha de pensamento doutrinadores, como o Professor Ramón Falcón y Tella, da *Universidad Complutense de Madrid*; e o Professor Rogério Greco, no Brasil, que também defende essa linha e que, na verdade, não é necessário, em absoluto, erigir normas específicas. Na verdade, e digo que muitas das observações que realizaremos ao longo do dia são da

mesma forma aplicáveis a outros ramos do Direito, além do Direito Tributário.

Arrisco-me a dizer que também no âmbito civil e no criminal não há a necessidade de se criar normas específicas para esse contexto telemático; não há por que criar, por exemplo, normas específicas para deter o cibercrime, por exemplo, ou para regular especificidades relativas ao contrato eletrônico. O mesmo ocorre em relação ao Direito Tributário.

O que há de se fazer – algo que comentava com o Presidente – é adaptar os institutos que já existem no Direito Tributário para que sejam aplicáveis a essa nova realidade, que é a relativa às operações telemáticas.

Essa seria uma primeira visão relativa ao plano normativo.

Uma segunda visão é aquela que defende a ideia de que, efetivamente, seria necessário construir um sistema tributário específico para essas operações, e o grande representante dessa corrente é o Professor Arthur Cordell, canadense, que escreveu um livro, talvez quem lida com essas questões tributárias certamente tenha conhecimento, propondo a instituição de um tributo específico que seria o *bit tax*; em outras palavras, um tributo que teria como fato gerador e como base de cálculo o volume de informações transferidas por meio da internet. Nesse caso, a depender do número de *bits* transmitidos, haveria uma tributação progressiva, uma tributação que equivaleria ao número de *bits*.

Existiriam outras propostas similares, pois, além do *bit tax,* temos, na doutrina, por exemplo, a tributação do *modem*. Há quem diga que seria necessário erigir um sistema tributário específico que deveria ter como objeto, sobretudo, as informações transmitidas por meio do *modem*. Há quem diga ainda que seria necessário especificar um tributo para as ligações telefônicas ou ligações via rádio, pelas quais são estabelecidas as conexões de internet.

O grande problema dessa corrente se dá, em primeiro lugar, em relação ao princípio da isonomia tributária e, em segundo lugar, talvez mais importante ainda, em relação ao princípio da capacidade econômica, que determina, em uma de suas facetas, expressar-se de diversas formas, conforme consta no art. 145 da Constituição Federal, que só deve haver incidência tributária onde existe riqueza, onde existe expressão de capacidade econômica.

Ora, o número de *bits* ou o volume de informações que se transfere por meio da internet não necessariamente indica a riqueza de quem está transferindo ou recebendo essa informação; e, aí, existe uma analogia feita pelo Professor Rogério Greco, no sentido de que um projeto de engenharia, um *software* extremamente avançado, que venha a ter um número de *bits* relativamente pequeno, seria muito pouco tributado em comparação, por exemplo, a uma transferência de informação que tivesse como objeto uma foto que é distribuída entre amigos de forma gratuita. Obviamente que, desde o ponto de vista do princípio da capacidade econômica, não teria qualquer consistência, seria absolutamente fragilizado o argumento da criação de um sistema tributário que tivesse um fundamento que não fosse o da riqueza da expressão da capacidade econômica.

Em relação ao argumento da isonomia, o que se alega é que não existiria subsídio para se promover um tratamento desigual entre as pessoas que estão realizando a mesma expressão de riqueza, que estão prestando o mesmo serviço, disponibilizando o mesmo bem e, em função apenas do meio através do qual estão realizando essas transferências, essas entregas, essas disponibilizações de serviços ou objetos, teriam um tratamento absolutamente distinto.

Em outras palavras, se saio, por exemplo, para comprar um *software*, aquele que o STJ chama de "*software* de prateleira", em uma loja, teria determinado regime tributário a ser aplicado sobre a minha pessoa e, caso venha a descarregar esse mesmo *software* diretamente

para o meu computador, teria outro regime tributário, outro tratamento tributário sendo aplicado sobre essa operação. Portanto, é a mesma operação, pelo menos do ponto de vista da sua essência. Entretanto, essa corrente doutrinária defenderia uma distinção de tratamento, que me parece absolutamente frágil, uma corrente doutrinária que se mostra extremamente fragilizada, principalmente com base em dois grandes argumentos: capacidade econômica e princípio de isonomia.

Existe uma terceira teoria, defendida pela Organização Mundial do Comércio (OMC), com interferência política dos Estados Unidos, que foi muito forte, sobretudo no advento da internet, em 1996, e, atualmente, encontra-se um pouco mais branda, que é aquela segundo a qual a internet deveria – e mais especificamente o comércio eletrônico – ser, na verdade, um universo absolutamente liberado, ou seja, isento de qualquer carga tributária. Obviamente que existia, por trás dessa corrente, um interesse político e econômico, já que – como sabemos – os Estados Unidos, pelo menos no início da internet eram, certamente, o grande exportador ou o grande produtor de tecnologia a ser disponibilizada por meio da própria internet.

Existem essas implicações, do ponto de vista do Direito Tributário material, mas são relativas ao plano normativo.

Ainda dentro do Direito Tributário material, temos aquilo que podemos chamar de implicações desde a perspectiva conceitual ou, se quisermos, em outra linha, desde a perspectiva institucional, mais especificamente acerca do entendimento que temos do que vem a ser os institutos de Direito Tributário. Nesse caso, eu dividiria, de novo, as implicações que têm a internet em dois grandes grupos: primeiro, no que diz respeito ao Direito Tributário material em relação aos conceitos, mais relativo à imposição direta sobre a renda e, mais especificamente, sobre o patrimônio.

A internet trouxe, também, a consequência de modificar ou de relativizar alguns entendimentos, que tínhamos anteriormente ao seu

advento, em relação a alguns institutos, como, por exemplo, o entendimento de que tínhamos, até o seu advento, sobre o chamado estabelecimento permanente, que era absolutamente distinto daquele que temos atualmente.

Retomarei a questão do estabelecimento permanente mais ao detalhe, aprofundarei um pouco mais a abordagem ao final desta palestra, mas só para termos uma ideia do que seja essa implicação, estabelecimento permanente sempre teve como conceito, dentro do Direito Tributário Internacional, de ser utilizado como referência para que possamos determinar de quem é a competência tributária no que diz respeito à incidência do Imposto de Renda no plano internacional.

Quando temos uma operação de pagamento de rendimento entre dois países, o que vige, o que se aplica, em geral, é o princípio da residência da renda, ou seja, será pago o Imposto de Renda ao país onde se encontra estabelecido o beneficiário desse pagamento. A ideia de estabelecimento permanente entra exatamente como um vetor, uma variável que indicará onde é que o indivíduo está estabelecido.

Até o advento da internet, o estabelecimento permanente era definido pelos modelos de tratados, sobretudo da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), entendido como a base fixa, a infraestrutura, o prédio onde funcionava determinada empresa.

O problema, a partir do advento da internet, é que esse estabelecimento, a partir do qual são organizadas as atividades econômicas, tornou-se absolutamente etéreo, sendo desnecessária a existência de uma infraestrutura física. Atualmente, pode-se ter um estabelecimento permanente em qualquer lugar do mundo, inclusive em um paraíso fiscal já que, no âmbito da internet, estamos falando, especialmente, de prestação de serviços e de disponibilização de bens imateriais.

Não é preciso ter uma fábrica, uma indústria na qual se terá o desenvolvimento de determinados serviços ou produtos; obviamente, o conceito, o entendimento que temos de estabelecimento permanente, após a internet, tem e vai sofrer algumas implicações, das quais falarei mais adiante.

Outra implicação, do ponto de vista conceitual, que é interessante, dá-se em relação aos *royalties* – e aí no que diz respeito à tributação do rendimento internacional; *royalty* é sempre um rendimento que se paga em função da disponibilização ou da exploração econômica de determinado bem, sobretudo, bens imateriais. A partir do advento da internet, o que houve foi uma ampliação do conceito de *royalty*. O universo daquilo que chamamos *royalty* modificou-se bastante.

Os tratados firmados pelo Brasil – atualmente, cerca de trinta – foram, em sua maioria, nas décadas de 70 e 80, sobretudo de 70. Ora, obviamente que o entendimento de *royalty,* quando o legislador tratou dele lá trás, era absolutamente distinto ou, pelo menos, o universo dos *royalties* era absolutamente distinto daquele que temos atualmente. Os bens imateriais produzidos a partir da digitalização dos objetos, das mercadorias, de uma forma geral, obviamente, fizeram mudar o entendimento que devemos ter em relação a esse tipo de rendimento.

Em relação à tributação indireta, ainda falando das questões conceituais, talvez os câmbios tenham sido ainda maiores. Por exemplo, até 1996 – e esse era o entendimento, inclusive, desta Corte –, até o aparecimento da internet, em meados da década de 90, o que tínhamos era que a distinção entre bem e serviço, que é uma distinção, do ponto de vista tributário importantíssima visto que determinará o pagamento do Imposto sobre Circulação de Mercadorias e Prestação de Serviços (ICMS) e do Imposto sobre Produtos Industrializados (IPI), por um lado ou por outro, o Imposto sobre Serviços de Qualquer Natureza (ISS), a distinção entre mercadoria e serviço, para efeito de tributação, sempre foi a questão da tangibilidade.

O STJ sempre entendeu – essa é a linha tradicional – que aquilo que for disponibilizado, o objeto que seja disponibilizado, dentro de uma transação econômica e que tenha natureza intangível, via de regra, será serviços e, portanto, objeto de incidência do ISS. Por outro lado, tudo aquilo que tenha uma natureza tangível será objeto de incidência de ICMS, por ser considerado mercadoria e, em alguns casos, produto industrializado, como o caso do *software*, por exemplo.

Então, obviamente, temos uma total modificação no que diz respeito ao entendimento do que vem a ser o objeto de uma transação comercial com repercussões importantes sobre a tributação indireta. Também faremos algumas considerações, ao final, mais específicas sobre esse tema. Falaremos do posicionamento atual do STJ, mas é importante, ao menos, para que entendamos o que é essa modificação de entendimento em função do advento das novas tecnologias da informação para o Direito Tributário.

Só para se ter uma ideia, ainda dentro dessa linha, tradicionalmente, a única mercadoria, para o Direito Tributário, que tinha natureza intangível, antes do surgimento da internet, era a energia elétrica, que, de fato, é até hoje considerada mercadoria, sem prejuízo da natureza jurídica que o Direito Civil, o Direito do Consumidor ou o Direito Administrativo determinem. A energia elétrica, para o Direito Tributário, por incrível que pareça, é uma mercadoria e não um serviço; portanto, será tributada no plano do ICMS.

Existe essa modificação de entendimento, essa implicação, como existe também uma implicação importante, uma modificação de entendimento ou, ao menos, uma discussão, em relação à distinção entre serviço de informação e serviço de comunicação. Tradicionalmente, outra vez, a distinção entre informação e comunicação se dá em função da nota da interatividade. Também é entendimento do STJ que a interatividade será própria do serviço de comunicação e, portanto, a comunicação, conforme determina o texto da Constituição de 1988, será objeto de

incidência do ICMS. Por outro lado, se não houver, na transmissão da mensagem, a nota da interatividade, ter-se-á um serviço de informação, que será objeto de incidência do ISS.

Essa é uma discussão que já existia mesmo antes da internet. A televisão é um serviço de comunicação ou seria de informação? O rádio é um serviço de informação ou de comunicação? A internet teve, nesse caso, a função de potencializar as discussões acerca da natureza jurídica de determinados serviços, enquanto informação ou comunicação mais específica e, especialmente, aos chamados provedores de acesso à internet, tema que retomaremos a tratar nesta palestra.

Apenas para entendermos, além desse primeiro grupo de implicações da internet sobre o Direito Tributário material, há o segundo grupo – e talvez seja, de todos, o mais importante, o mais significativo –, de que seriam as várias modificações, as várias implicações que teve a internet, que tiveram as novas tecnologias da informação sobre o Direito Tributário formal e, nesse caso, estaríamos nos referindo àquilo que o Código Tributário Nacional chama, equivocadamente, segundo a doutrina, de obrigações tributárias formais ou acessórias.

Nesse caso, quais são ou foram as implicações, no Direito Tributário, no que diz respeito à gestão de tributos, à fiscalização de tributos, ao controle, de uma forma geral, dos tributos? Foram várias as implicações. Primeiro, as relativas à comunicação entre a administração tributária e os contribuintes. Nesse caso, houve uma verdadeira revolução, mormente, naqueles casos em que tratamos da utilização do *e-mail* enquanto um canal de comunicação entre as administrações tributárias e, por outro lado, os contribuintes. Foi, de fato, uma implicação, uma modificação de grande impacto na administração tributária.

Também houve, do ponto de vista formal, uma modificação na via contrária, na via inversa, ou seja, da comunicação entre contribuinte e administrações tributárias de uma forma geral, com importantes

implicações e conseqüências, de outro lado, sobre a questão do sigilo e da privacidade dos indivíduos de uma forma geral.

Nesse caso, é interessante estudar o Direito Tributário formal brasileiro após o advento da internet. Temos, no Brasil, o que há de mais avançado em termos de tecnologias da informação aplicada ao Direito Tributário, estamos na vanguarda em vários aspectos e bastante atrasados; dentro do próprio sistema tributário brasileiro, temos, portanto, essa dicotomia.

Temos uma Receita Federal, por exemplo, que é elogiada e se encontra entre as melhores do mundo – é citada ao lado da Austrália, da Espanha e do Canadá como uma instância administrativa tributária de primeira grandeza, de modernidade bastante pronunciada e temos, por outro lado, os municípios brasileiros, o interior do Brasil.

No interior do Brasil – e posso falar com bastante tranquilidade, porque tenho atuado exatamente na linha de modernização, de inclusão digital das fazendas públicas municipais –, o que é interessante, nos municípios brasileiros – e estamos falando de um tema extremamente avançado, de novas tecnologias aplicadas à tributação –, como no interior da Bahia, não temos, sequer, na grande maioria, a existência de um código tributário municipal.

A grande maioria dos municípios na Bahia, quando tem um código tributário municipal, é, inclusive, anterior a 1988, à própria Constituição Federal, o que é algo interessante, porque, ao mesmo tempo, temos um processo de fusão da Receita Federal com o Instituto Nacional do Seguro Social (INSS); temos a Empresa de Tecnologia e Informações da Previdência Social (Dataprev) e a própria página do INSS, que dá uma perspectiva de que, em médio prazo – e isso já vem sendo anunciado, como todos devem saber –, não teremos mais que enviar informações à Receita Federal, pois terá um nível de informação, em função da fusão entre o INSS e a Receita Federal, acerca dos contribuintes, o que permitirá o envio, a cada um deles, do que é a sua renda anual e, com

base nisso, o cálculo do próprio Imposto de Renda para que, simplesmente, se vá a uma agência bancária realizar o pagamento.

Nos âmbitos federal e estadual, por exemplo, há a possibilidade de lançar o Cadastro Nacional da Pessoa Jurídica (CNPJ) de determinada empresa, imprimir a certidão negativa e participar de qualquer processo licitatório, mas é verdade que existem, ainda, algumas lacunas.

Atualmente, no Brasil, para participar de uma licitação, é necessário que o indivíduo corra atrás de, nada menos, do que cinco certidões negativas. É verdade que, ao acessar a página da Caixa Econômica Federal, retira-se a certidão negativa de FGTS; ao acessar a página do INSS, retira-se a certidão de contribuições previdenciárias; na Receita Federal, retira-se a dos impostos ou dos tributos federais de uma forma geral; e, finalmente, ao acessar as páginas das secretarias estaduais da fazenda, retira-se, também, na maioria dos casos e de forma gratuita e eletrônica, a certidão negativa.

O grande gargalo, o problema da administração tributária brasileira encontra-se, entretanto, pelo menos do ponto de vista dos procedimentos formais, nas fazendas públicas municipais. A fazenda pública municipal, por mais contraditório que possa parecer, é exatamente aquela que mais emperra o desenvolvimento das micro e pequenas empresas ou das empresas, de forma geral, instaladas no próprio território municipal.

Atualmente, na grande maioria dos municípios do interior do Brasil, o indivíduo tem de protocolar um pedido formal – e estamos na era da informática, da internet –, por escrito, a fim de que, em 48 horas, ou 5 dias, se der sorte de o secretário municipal de fazenda ou o indivíduo com poder delegado, para emitir a certidão, estar no município, seja emitida essa certidão negativa e possa participar, por exemplo, de um processo licitatório, algo extremamente oneroso, contraproducente, contrário aos próprios interesses do município.

É interessante e contraditório porque, se uma empresa está estabelecida no município do interior do Brasil e queira participar de um processo licitatório a se realizar em São Paulo ou Salvador, mas, simplesmente, fique impedida de participar, porque o próprio município, o grande interessado e beneficiário dessa prestação de serviços, teria em seu favor o pagamento do ISS, impede essa empresa de participar desse processo por não ter as ferramentas básicas, elementares, a fim de possibilitar a participação nesse certame.

É interessante, como havia dito, o que é a dicotomia entre o âmbito federal e o estadual na utilização das novas tecnologias da informação aplicadas ao Direito Tributário e, por outro lado, à realidade de todo interior do Brasil.

É verdade também que, a partir de 2008, se tem desenvolvido uma rede nacional, a chamada "Rede Sim", que está sendo pensada, projetada para incluir a vida de todas as empresas, todos os CNPJ's, em todos os âmbitos da administração brasileira. Em outras palavras, tal rede unificará todos os procedimentos que estamos falando, principalmente, das certidões negativas.

A empresa apenas deverá enviar ou preencher seu CNPJ e terá seu histórico econômico-tributário tanto no âmbito federal como no municipal e estadual. Nesse caso, haverá informações importantes, como as declarações de todo tipo e não somente a específica de rendimentos, mas as relativas aos pagamentos que as empresas realizam. É nesse sentido que estávamos falando. A Receita Federal possui um nível de informação, atualmente, que lhe possibilita inclusive calcular o tributo sem haver a necessidade de o contribuinte aportar nenhuma informação adicional.

Na Espanha, tem-se discutido muito a esse respeito. Em um simpósio internacional de que participei, especificamente naqueles cursos de verão em El Escorial, Madrid, chamou-me a atenção um sistema que está sendo implantado na Espanha denominado Sistema *Full Hard*, que é muito interessante – o representante da Fazenda Pública espanhola falou

a respeito dele com os olhos brilhando –, mas assustou-me muito esse Sistema, principalmente, com vistas à questão do sigilo e da privacidade.

O *Sistema Full Hard*, segundo explicações do representante, dentro de pouco tempo, possibilitará à Fazenda Pública espanhola ter todo o perfil do que seria um fraudador, inclusive o perfil físico, pois possibilitará saber quantos filhos o indivíduo possui, qual o seu tipo físico etc. Foram palavras dele: "Se o indivíduo seria loiro ou moreno, se teria olhos azuis ou olhos verdes". Falou como se fosse uma grande conquista da Fazenda Pública espanhola.

Obviamente, o nível de controle que se terá a partir dessas informações é muito grande, mas é temerário, assustador, especialmente do ponto de vista dos direitos e das garantias individuais fundamentais.

Mesmo no Brasil, temos caminhado nessa direção. Se alguém tinha dúvida acerca da privacidade, do sigilo que se possa ter das informações da internet, certamente, pode tirá-las, porque é verdade. A Receita Federal, por exemplo, tem todas as ferramentas possíveis para obter a sua movimentação bancária, acessar seu *e-mail* e, absolutamente, qualquer que seja a informação, inclusive senhas bancárias.

Ainda no Direito Tributário formal, existe a questão do processo eletrônico, que também é uma realidade. Na Bahia, infelizmente, estamos bastante atrasados, porque estamos iniciando a etapa de digitalização dos processos. Essa é uma realidade geral não só aplicada ao Direito Tributário, mas a todos os âmbitos do Direito. Temos vivenciado essa realidade, principalmente nos Estados do Sul, no Paraná, no Rio Grande do Sul e em Brasília, mas é também um processo inevitável que o Direito Tributário deve ser incluído nessa realidade.

Finalmente, dentro da questão do Direito Tributário formal, o intercâmbio de informações entre administrações tributárias, ao arrepio dos direitos e das garantias individuais fundamentais, vem sendo cada vez mais utilizado.

São essas as medidas que vêm sendo tomadas no Direito Tributário formal, e diria que as principais discussões a serem fomentadas são, principalmente, no que diz respeito aos direitos fundamentais de sigilo e privacidade da pessoa humana, do cidadão.

Finalmente, o terceiro grupo de implicações do Direito Tributário, como tínhamos anunciado anteriormente, diria que se refere especificamente ao controle das operações eletrônicas, das operações de comércio eletrônico.

Uma coisa é a implicação sobre o Direito Tributário material e o Direito Tributário formal, outra é saber como será feita a fiscalização de uma operação que se dá na sua integridade e integralidade por meios telemáticos.

Nesse caso, cabe uma observação importante: ao falarmos em comércio eletrônico, para efeito de controle tributário, estamos falando daquela operação realizada pela internet na sua inteireza, ou seja, não é a realizada em parte por meio da internet. Aquela operação na qual se adquire, por exemplo, um computador, um programa de computador, ou um livro que vem de outro Estado, ou seja, quando se adquire um bem tangível por meio da internet, essa operação apresenta-se pouco interessante e importante do ponto de vista do controle tributário. É uma operação similar e idêntica, para efeito de controle tributário, àquela que realizamos ou que realizaram nossos avós, as chamadas compras por catálogo. Ao comprar um computador ou um bem tangível por meio da internet, o controle a ser dado nessa operação é exatamente igual ao que se dá em qualquer operação tradicional. A única diferença é que o pedido foi feito por meio telemático.

Outra situação é o controle tributário que se vai estabelecer naquelas operações, na sua totalidade, realizadas por meio da internet, as quais são importantes para efeito de estudo, verificação e consideração das medidas de controle tributário. É o caso, por exemplo, do indivíduo que não adquire o CD, mas, na verdade, adquire a música diretamente da

internet, baixa de determinado provedor, determinada página da internet, direto para o seu computador.

Poderia ser uma música com valor agregado muito pequeno ou um programa de computador que não teria uma grande importância, relevância, do ponto de vista econômico, mas poderia ser também um programa de engenharia, um programa de gestão empresarial, que vai ter uma importância econômica extremamente elevada. Exatamente em relação a tal operação que se estabelecem os problemas relativos ao controle tributário. Nesse caso, as fazendas públicas, de forma geral, não possuem, ainda, as ferramentas que seriam necessárias para realizar um controle tributário efetivo. Elas não têm todos aqueles padrões, pontos de interseção, do comércio tradicional.

Não é como se fiscalizar uma operação com um CD em suporte material. No caso do CD, existe a empresa que o fabrica, o transportador e os vários intermediários da operação, podendo-se exigir informação a cada um desses intermediários. Na internet, não. Nesse caso, há a supressão de um grande número de intermediários ou, por outro lado, a modificação desses intermediários.

O mais importante seria a adequação do controle tributário para esse novo cenário virtual. Não há um caminhoneiro que vai realizar o deslocamento da mercadoria, levar a mercadoria de um local a outro, mas existe uma série de intermediários que podem servir como pontos de apoio para a fiscalização tributária.

Há o provedor, o servidor de rede, as instituições financeiras de uma forma geral, as empresas que têm as bandeiras de cartões de pagamento, sejam de débito ou crédito, mas o mais importante é que as fazendas públicas venham a se adequar de forma a terem a possibilidade de fiscalizar esse novo cenário que se apresenta para a fiscalização e o controle dos tributos no âmbito telemático.

De uma forma geral e sem prejuízo de algumas considerações mais específicas que vamos realizar, diria que, de forma sistematizada, seriam esses três os grandes grupos de implicação da internet sobre o Direito Tributário.

Como falei anteriormente, acredito que, em grande medida, essas mesmas implicações, com as devidas especificidades a cada ramo do Direito, também, nos demais ramos do Direito, vão se apresentar dessa forma: vão relativizar conceitos, mudar entendimentos acerca de determinados institutos e modificar a nossa ideia acerca do que venham a ser os procedimentos. Diria que vêm para melhor, para agilizar os procedimentos de uma forma geral e, também, fazer com que a estrutura administrativa do Estado torne-se adequada de forma a poder prover o controle e a fiscalização das muitas operações.

Falando de forma mais específica, pragmática e aplicada, é verdade que seriam muitas as questões a serem trazidas à discussão, mas chamaria a atenção para três relacionadas ao Direito Tributário que estão, inclusive, sendo discutidas nos tribunais.

A primeira refere-se, como foi dito no início, à questão do estabelecimento permanente que, por sua vez, é um conceito extremamente importante para a definição da competência tributária em matéria de imposição sobre a renda no âmbito internacional.

O que existe, hoje, em conflito de competência, em matéria de imposto de renda? Obviamente que, tratando-se o imposto de renda de um imposto de competência federal, não poderia deixar de ser um conflito internacional. O Estado, o município, no Brasil, não tem competência para exigir o pagamento do imposto de renda e, obviamente, não vai haver conflito entre o Estado, o município e a União acerca da tributação sobre a renda. Esse conflito, portanto, vai ser internacional.

Seria o caso de uma empresa estabelecida no Brasil, que fabrica *software*, que produz *software*, e vende a sua produção para os Estados

Unidos, a Espanha ou a França. Nesse caso, o rendimento será tributado pelo Brasil, pela Espanha ou pelos Estados Unidos? É essa a discussão.

Em geral, e poderíamos utilizar o termo tradicionalmente, esses conflitos são resolvidos por meio da aplicação dos chamados convênios bilaterais para evitar a bitributação e a evasão fiscal internacional. Em geral, aplicam-se as normas dos convênios firmados de forma bilateral.

O que são esses convênios? Grosso modo, são normas que determinarão, basicamente, duas medidas: primeiro, determinarão a classificação dos muitos rendimentos que podem existir entre dois países. Então, haverá, e de fato há, nos cerca de trinta artigos colocados nesses convênios, uma classificação de todos os rendimentos possíveis entre, por exemplo, o Brasil e a Espanha, que resolveram especificar que os rendimentos objeto de tratamento do convênio serão tais e quais, em que se terá juros sobre capital próprio, *royalties*, ganho de capital, aluguel, rendimento de salário e assim por diante. Nesse caso, essa seria a primeira medida, como dito: a classificação dos muitos rendimentos que vão interessar essa relação bilateral.

Existe outro grupo de medidas que seria a eleição, a escolha do critério que será aplicado para cada um desses tipos de rendimentos que foram escolhidos e indicados pelo próprio tratado.

Em geral, sem prejuízo de outros critérios indicados, há basicamente dois: ou o da fonte ou o da residência. O critério da fonte é aquele, segundo o qual, quem terá a competência para tributar é o país de onde se origina o pagamento. Se a empresa está no Brasil e remete seus lucros para fora, escolhendo-se, nesse caso específico, o critério da fonte, a competência seria do Brasil, já que é daqui que sai o rendimento pago.

Pelo critério da residência, por outro lado, ocorreria exatamente o inverso, ou seja, será competente o país em cujo território esteja radicado o beneficiário desse pagamento.

Em regra, o critério adotado pela grande maioria dos países, pela grande maioria dos tratados firmados é o da residência, ou seja, o critério pelo qual quem vai ter competência para cobrar o imposto de renda é o país no qual está localizado o beneficiário desse rendimento, e é aí, exatamente, que entra a ideia do estabelecimento permanente. Sabemos que é o critério da residência, o critério onde está localizado o beneficiário do pagamento. Mas quais são os critérios técnicos, as circunstâncias materiais que me farão identificar onde está localizada a empresa? Nesse caso, os tratados costumam adotar o conceito de estabelecimento permanente. Em outras palavras, será o local onde a empresa tenha o seu estabelecimento.

Segundo esses mesmos tratados, a ideia do estabelecimento permanente é a que está intimamente ligada à questão da infraestrutura. É interessante que, no Direito brasileiro, tanto no Direito Civil como no Direito Tributário – e foi algo que discutimos em Salvador, ao promovermos um seminário com professores espanhóis, há duas semanas, no qual um dos professores fez muito bem, exatamente, tal observação –, por incrível que pareça, no Brasil, a legislação nacional sequer cita o que vem a ser estabelecimento permanente, embora seja um conceito que adotamos em todos os tratados firmados, são cerca de trinta tratados firmados com outras nações.

O Código Tributário Nacional, por exemplo, adota o critério de domicílio de eleição, conforme o art. 127 do Código Tributário Nacional. Em nenhum momento, há uma referência ao que seria estabelecimento permanente. O Código Civil, no art. 75, determina que, na verdade, não há estabelecimento permanente, há o domicílio da empresa, que será a sede da empresa ou o local onde são tomadas as decisões empresariais.

Portanto, a própria definição de estabelecimento permanente, para efeito de incidência do imposto de renda nas transações internacionais, é dada apenas pelos próprios convênios. O estabelecimento permanente para os convênios é a infraestrutura física, nesses termos que é tratado

nos convênios bilaterais para evitar a bitributação e a evasão fiscal internacional.

Qual o problema em relação ao advento da internet? É que a própria dinâmica econômica, em função da própria natureza dos bens disponibilizados por meio da internet, não necessita, não demanda a existência desses estabelecimentos físicos, que podem ser alocados em qualquer parte do mundo. Aliás, conforme indica a doutrina, podem, inclusive, ser identificados com um *notebook*, um equipamento que seja móvel, não precisa haver uma estrutura física para se fabricar ou para se elaborar um *software*.

Obviamente, temos, nesse caso, um grande problema: se sabemos que vai ser o critério da residência a determinar a competência tributária, qual o critério prático para se dizer onde está estabelecido um indivíduo que elabora um *software*, visto que essa empresa, sequer, tem uma residência e um endereço físico? Mais que isso, é um indivíduo que elabora *software* e pode estar localizado em qualquer parte do mundo, pode localizar a sua empresa, sua página virtual, inclusive, em um servidor de rede que esteja localizado, por sua vez, em um paraíso fiscal.

Ora, se localiza ou coloca sua página a partir de um servidor localizado em um paraíso fiscal ou em um país que tenha um regime tributário mais benéfico, obviamente que, pelo critério da residência, adotado pelos modelos de tratados de uma forma geral, esse indivíduo teria que ser tributado nesse país, embora saibamos que, na prática, nem vai ser elaborado o *software* naquele país, nem as operações de comercialização serão realizadas naquele mesmo país em que alega estar estabelecido.

Em segundo lugar – e essa é uma questão que o STJ foi chamado a julgar –, outra questão específica e interessante diz respeito à tributação do software – e estamos falando em tributação indireta, tributação de ISS, ICMS, IPI, Contribuição para o Financiamento da Seguridade Social (Cofins) e PIS. Nesse caso, o que se coloca é o seguinte: anteriormente,

falamos que, tradicionalmente, a distinção entre serviço e mercadoria é extremamente importante do ponto de vista tributário. A depender de como se classifica determinado objeto, haverá a incidência do ISS; se classificar como serviço, por outro lado, haverá a possibilidade, também, de determinar a incidência de ICMS e IPI.

Do ponto de vista econômico, apenas para termos uma ideia do que seria o impacto econômico disso, vai-se sair de uma possibilidade de tributação que varia de 2% a 5%, no regime do ISS, para uma tributação que pode ser superior inclusive a 300%, já que estamos falando de IPI, já que o *software* é um produto industrializado, como também do ICMS, que, em geral, vai ter alíquotas variando entre 17% e 18%, a depender do estado. Nesse caso, o impacto econômico é, de fato, muito importante.

Tradicionalmente, o serviço, segundo o STJ, é um objeto intangível; a mercadoria vai ser, por outro lado, um objeto tangível. Há a exceção, como citado, da energia elétrica, que seria uma mercadoria intangível.

O grande problema, a partir da internet, é exatamente o processo de informatização, de digitalização e, portanto, da transformação de determinados bens que, até então, eram considerados tangíveis em bens intangíveis por excelência. Seria o caso, por exemplo, das obras musicais, do livro e dos programas de computador, de uma forma geral, que não estão disponibilizados em determinada loja, em determinada embalagem material, mas por meio do computador.

Instaurou-se, durante toda a década de 90, exatamente, uma discussão sobre se haveria de ser a tributação em matéria de ICMS ou de ISS. O STJ veio a ser chamado a julgar, o que foi interessante, porque, até o final da década de 90, uma das Turmas alegou que o *software* se tratava de um serviço e outra entendeu que, na verdade, estaríamos diante de uma mercadoria e, portanto, deveria ter o tratamento tributário específico, próprio do que seria uma operação com mercadoria.

Obviamente, existem algumas implicações no que diz respeito ao princípio da isonomia, pois não tem sentido se comprar determinado *software* em uma loja e ser tributado no regime de ICMS, e se comprar, por outro lado, o mesmo *software*, mas diretamente do seu produtor, do seu elaborador, da página que o produziu. Em função apenas da forma por meio do qual se adquiriu o programa, tem-se um tratamento tributário absolutamente distinto. Do ponto de vista do princípio da isonomia, obviamente, seria algo insustentável.

Nesse caso, o STJ desenvolveu um entendimento posterior, ainda no final da década de 90, início do ano 2000, segundo o qual, o critério para definir se será serviço ou mercadoria deixaria de ser o da tangibilidade, abandonaria o critério tradicional e passaria a adotar outro, que é a finalidade comercial ou econômica que terá esse *software*. Portanto, a distinção feita pelo STJ foi no sentido de afirmar: se for um *software* elaborado para atender necessidades específicas de determinado indivíduo ou de determinado grupo de indivíduos, o que o próprio STJ chamou de *software* sob encomenda, elaborado sob encomenda, nesse caso, teríamos uma operação com serviço, um serviço **intuito personae** e, portanto, não teria motivo de ser classificado de outra forma, nesse caso, a tributação seria no regime do ISS.

Por outro lado, o *software* que, muito embora fosse disponibilizado de forma intangível, mas disponibilizado para o mercado de uma forma geral, aquilo que o STJ chamou de *software* de prateleira, voltado para o mercado sem distinção do seu beneficiário, será considerado, na verdade, uma mercadoria e, portanto, será tributado como tal, tanto no regime do ICMS, como no regime do IPI.

Ainda em relação ao *software,* existe outra discussão interessante que terá uma repercussão desde a perspectiva da tributação internacional, que é a questão de saber qual a natureza do serviço prestado. Os modelos de convênio de uma forma geral, e é outra questão que, certamente, será enfrentada pelos tribunais, fazem uma distinção entre *softwares* técnicos

ou científicos e *softwares* que são programas de computador, artísticos ou culturais, que determinam um regime tributário, tanto no que diz respeito à competência do país como no que diz respeito à alíquota a ser aplicada, absolutamente distinta da discussão que os tribunais serão chamados a dar o seu posicionamento.

Finalmente, a última questão para a qual chamo a atenção de todos é relativa ao tratamento tributário dos chamados provedores de acesso à internet, que é também outra questão que o STJ teve a oportunidade de tratar e julgar.

As questões relativas aos provedores de acesso à internet estão dentro daquele grupo de discussões que tratamos anteriormente, sobre saber se estamos diante de, sem dúvida, um serviço, mas, nesse caso, seria a discussão em torno de saber se se trata de um serviço de comunicação ou um serviço de informação.

Nesse caso, também foi muito interessante o posicionamento do STJ. Houve muita discussão em um primeiro momento; houve quem afirmasse que, na verdade, o provedor de acesso à internet possibilita a comunicação; portanto, possibilitando a comunicação, ensejando a comunicação, deveria ser objeto de incidência do ICMS, e haveria interatividade entre os sujeitos.

Houve quem afirmasse que, na verdade, o provedor de acesso à internet é apenas um serviço de informação e, portanto, objeto de incidência do imposto municipal, o ISS.

Houve, ainda, uma terceira via interessante, a qual o STJ terminou pendendo de forma mais pronunciada, qual seja a classificação do provedor de acesso à internet como sendo um serviço **sui generis**, nem é serviço de comunicação, nem de informação, mas, na verdade, palavras do próprio STJ, adicionado ao serviço de comunicação. Há um serviço de comunicação, que, em um primeiro momento, no caso da internet era

feito por meio de telefone, e àquele serviço de comunicação adicionou-se um segundo, o serviço de possibilitar o acesso à internet.

Como um serviço **sui generis**, autônomo, que se coloca acima do serviço de comunicação, que utiliza o serviço de comunicação como infraestrutura, se você tentar enquadrá-lo, obviamente, só poderá enquadrá-lo no ISS; o que acontecia, num primeiro momento, é que se tinha caracterizado diante de si o instituto da não incidência, em outras palavras, é um serviço a mais, um serviço que não existia, que não havia a sua previsão na lista anexa do Decreto-Lei nº 406, de 1964, e, portanto, sendo um serviço autônomo, que não está previsto na lista anexa e em respeito ao princípio da tipicidade ou tipologia cerrada, tal como ocorre no Direito Penal, como não há previsão expressa desse serviço, não poderia ser objeto de incidência sequer do ISS.

É verdade que, atualmente, tivemos reformas na legislação do ISS e houve a inclusão, também, dos provedores de acesso à internet como um serviço **sui generis**, autônomo e específico, que deverá ser objeto de incidência do imposto municipal.

Essas são as considerações que faria, pelo menos inicialmente, pois não sei como está o desenho deste evento, mas, de toda forma, dou por encerrada a minha primeira participação e fico à disposição daqueles que tenham eventuais dúvidas a serem levantadas.

Muito obrigado.

CLÁUDIA AUSTREGÉSILO DE ATHAYDE BECK
Secretária dos Órgãos Julgadores

Há uma questão, não sei se está contextualizada na sua palestra, mas uma dúvida que tem assolado os meios jurídicos, pelo menos a discussão no Tribunal tem sido grande, é relativa ao recolhimento do porte de remessa e retorno do processo eletrônico, uma vez que os especialistas em informática dizem que não é gratuito o tráfico de informações informatizadas. De que forma essa discussão tem sido abordada no meio jurídico?

ANDRÉ ALVES PORTELLA

Professor

De fato, a discussão que se levanta é relativa à devolução do porte de remessa e de retorno dos recursos. Nesse caso, o não pagamento desses portes é em função de estarem sendo transmitidos por meio da internet.

A colega está levantando a questão relativa à gratuidade, às discussões inerentes à gratuidade dessas taxas cobradas em função da ida e do retorno dos recursos aos tribunais.

Não temos, ao menos no âmbito tributário, levantado essa discussão. Envolveria, como você está falando, uma questão de técnica de informática, mais especificamente, haveria, como você falou, um custo para ser realizado, mesmo sendo por meio da digitalização, o envio da informação. Do ponto de vista tributário o que poderia ser discutido nesse caso seria, talvez, a natureza jurídica, se bem que não seria uma discussão, pelo menos no âmbito tributário, tão polêmica, visto que se trataria de uma taxa, como a de preparo e a atual taxa de remessa em suporte normal.

Diria que, juridicamente, não sei se haveria polêmica quanto a isso, do ponto de vista técnico, pois penso que seria muito mais uma questão de política judiciária de saber se se deve ou não cobrar essa quantia.

Muito obrigado.

Bom, para não constranger o público, pois estamos numa quinta-feira chuvosa – aliás, não sei se a chuva foi boa ou ruim, já que talvez o raciocínio tivesse sido esperar ela passar para não ter o problema de pegar uma enxurrada –reitero as palavras já pronunciadas. Meu agradecimento. E fico muito lisonjeado do convite que me foi feito, verdadeiramente, sobretudo, por saber da qualificação técnica do público presente.

Obrigado e dou por encerrado, portanto, essa palestra.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Senhoras e senhores, bom-dia!

O Seminário de Direito Eletrônico é uma iniciativa do Superior Tribunal de Justiça e do Instituto dos Magistrados do Distrito Federal – IMAG-DF e tem como proposta: ministrar conhecimentos básicos e especializados sobre o Direito Eletrônico para aprimoramento de servidores; ampliar a capacidade de interpretação das questões jurídicas surgidas no desempenho das funções exercidas; possibilitar a identificação das possíveis soluções jurídicas para os casos concretos; e capacitar o participante à melhor utilização da terminologia técnico-científica do Direito nas atividades funcionais.

Iniciaremos os trabalhos do segundo dia com a palestra *Propriedade Imaterial do Direito Eletrônico*. Para proferi-la, convidamos o Dr. Hildebrando Pontes Neto, graduado pela Universidade Federal de Minas Gerais; atualmente, é professor da Faculdade de Direito Milton Campos e também da UNA – Centro Universitário; é chefe de departamento de disciplinas básicas e complementares da Faculdade de Direito Milton Campos; tem experiência na área de Direito, com ênfase em direito autoral, atuando principalmente nos seguintes temas: direito de propriedade, concorrência desleal, propriedade intelectual, plágio e direito de autor.

Com a palavra o Dr. Hildebrando Pontes Neto.

PALESTRA V: PROPRIEDADE IMATERIAL DO DIREITO ELETRÔNICO

HILDEBRANDO PONTES NETO
Professor da Faculdade de Direito Milton Campos
UNA Centro Universitário

Em primeiro lugar, peço desculpas aos senhores, porque era minha intenção trazer uma exposição eletrônica, mas não tive condições de fazê-lo, porque fui acometido de uma febre há dois dias, o que não me impedirá evidentemente de lançar reflexões em torno do tema e quiçá propiciar a discussão e o debate.

Antes de qualquer coisa, gostaria de declarar minha enorme satisfação, da forma como me sinto prestigiado, porque considero extremamente honroso poder estar aqui a convite do Instituto dos Magistrados do Distrito Federal, conglobando as principais cortes de justiça do nosso País. Agradeço ao convite na pessoa do Desembargador Valter Xavier. Muito obrigado pelo convite.

Devo dizer que, ao refletir sobre o tema que me foi proposto, parti de uma visão prática para estabelecer exatamente o ponto de contradição, de debate, de dificuldade que hoje a propriedade intelectual alcança, em função das novas tecnologias, porque, sabidamente, quanto mais avançam as tecnologias, mais distante da criação fica o criador, e os reflexos daí não são de fácil tratativa, de fácil percepção, de fácil compreensão e de fácil equação. Se verificarmos a legislação existente no País, do Império para cá, compreenderemos que o direito de autor sempre foi fonte primeira nas nossas constituições, exceto a Constituição de 1937, além do que essa legislação estava premida no antigo Código Civil de 1916, entre o direito das obrigações e das coisas, quando veio a Lei nº 5.988, de 14/12/1973 e retirou do âmbito do Código Civil o direito de autor, propiciando que ele caminhasse com suas próprias pernas.

A partir daí, só viemos ter uma modificação em 1998, com a Lei nº 9.610, de 19/02/1998. Significa dizer, portanto, que, do ponto de vista legislativo, o Brasil tem protegido os direitos autorais e também o direito

de propriedade industrial, que tem uma legislação própria. Além disso, é signatário dos principais tratados internacionais ligados à área. Mas a sociedade é profundamente dinâmica e reputo como transformação fundamental, essencial, as que passaram a ocorrer na década de 40 do século que se findou, quando surge a informática e, por meio de um desenvolvimento avassalador, veio em cascata a criação de tecnologias que vão permitindo uma nova maneira de utilização de apropriação das criações intelectuais, genericamente tomadas.

O outro aspecto que reputo fundamental é que não existia até então estudos econômicos para indicar o que representava a propriedade intelectual do ponto de vista do PIB dos países desenvolvidos e em desenvolvimento. Esses estudos econômicos revelaram a importância econômica da propriedade intelectual de tal molde a despertar nos países ou nas sociedades internacionais a importância e o significado econômico desse direito.

Quero deixar claro que quando falo de propriedade intelectual, da qual o direito de autor é espécie, a propriedade industrial e outras criações que não vão tendo acomodação nos institutos já preexistentes e que vão ganhando espaço nessa construção, faço-o de uma maneira genérica. Há uma expressão muito feliz de um tratadista espanhol chamado Hermenegildo Baylos em que ele diz que, por força dessa evolução e dessa circunstância, a propriedade intelectual tornou-se um grande espaço jurídico. Mas importa dizer que a partir do momento em que se despertou para os interesses econômicos, que subjazem a evolução e a dialética do processo de propriedade intelectual, os países passaram a ter uma maior atenção com relação a essa questão.

A lei brasileira de 1998, que tramitou por mais de dez anos e, evidentemente, propiciou um grande debate junto aos principais segmentos de criação intelectual do País, no sentido de que esses segmentos pudessem ofertar as suas contribuições, seus reclamos e as suas reivindicações, tornou-se um diploma de certa feita moderno, atual e

que já nessa altura merece pontuadamente algum tipo de transformação, em que pese a sua estrutura sistêmica como um todo, considero-a como sendo uma boa lei. Mas quero pontuar com isso que os principais institutos que solidificaram o direito de autor, que é exatamente o direito moral de autor e o direito patrimonial de autor, que são os dois pilares que sustentam a construção arquitetônica autoral, permanecem em consonância com as principais legislações do mundo contemporâneo.

E o Brasil ainda foi beneficiado porque, quando veio a discussão do Tratado de Trips, a questão foi deslocada do âmbito da OMP para a OMC – e esse deslocar já demonstra uma preocupação de ordem econômica com a questão da propriedade intelectual. Em 1994, com a Rodada Uruguai, foi fechado o Tratado, e os países signatários ficaram com a obrigatoriedade de adequar-se ao Tratado de Trips, alterando a sua legislação. Como o Brasil vinha discutindo e debatendo a lei no Congresso Nacional, foi possível, exatamente por essa dilatação de prazo, que pudéssemos adequar a nossa legislação aos principais pressupostos do tratado. Significa dizer que, na comemoração dos 300 anos de direito de autor, o Brasil se ajusta a uma legislação internacional, quero crer, de uma forma harmônica.

Essa observação genérica, apenas descrevendo o cenário onde penso pontuar a minha reflexão, deve-se à dicotomia que se coloca hoje. Por um lado, os mecanismos eletrônicos – e, dentro deles, o mais expressivo é a internet, esse meio de comunicação e de negócio, talvez mais perfeito e mais plural que a sociedade humana tenha produzido –, e, de outro, a criação de uma multiplicidade de autores, que, ou por espontânea determinação e vontade, colocam nas esteiras eletrônicas as suas criações, e é um direito absolutamente sagrado, não há o que discutir sobre isso, e aqueles que resistem em permitir que o produto da sua criação seja forçosamente um resultado da cultura do remix.

Quero deixar uma reflexão que me parece fundamental. O grande problema da propriedade intelectual, em especial do direito de autor,

reside ainda na discussão do que significa ideia e forma de expressão. Esse, do meu ponto de vista, é o aspecto nevrálgico, essencial a nortear essa discussão.

A pugna que se trava conceitualmente entre ideia e forma de expressão é que permitirá compreender o porquê de uma resistência e o porquê da intenção de destruir essa resistência para que se possa apropriar dessas obras sem mais aquela.

Independentemente de teóricos como Hugo Grossius, John Locke, que é o grande pensador dessa questão, das questões que se travaram no direito americano, o fato é que John Locke, do meu ponto de vista, coloca a questão de uma maneira palatável. Qual a sua reflexão? Por que ele entende que é um direito de propriedade? Porque ele entende que é um labor intelectual, e que as ideias estão no *commons*, no domínio público. Mas, a partir do momento em que qualquer um de nós, pela inteligência, sensibilidade e percepção de mundo, dá a esta ideia uma forma de expressão, agregou a esta realização um contributo pessoal e, por isso mesmo, deve ser respeitado e protegido. Principalmente, quando se verifica que esses autores vivem do resultado e do produto da sua própria concepção.

E mais, na medida em que um autor dá forma de expressão a essa ideia, não retira dela a possibilidade de que ela reflita ideias novas, e que esse autor possa se valer dessas novas ideias para continuar o processo de criação. Penso que essa colocação é de uma clareza solar e não tenho dificuldade nenhuma em compreender isso. De igual sorte, não tenho por que criticar quem pretende disponibilizar a sua criação na esteira eletrônica, na rede, ou seja, quem pretende comunicar o seu labor ao mundo, assim como também entendo que aquele que assim não o pretende fazer deve ser respeitado e resguardado.

O grande ponto de debate que se trava é exatamente em torno dessa questão. Contrariamente a essa postura, vem um movimento alienígena chamado *creative commons*, em que um professor de *Stanford*,

um constitucionalista, por que perdeu uma demanda judicial contra a Disney, nos Estados Unidos da América, resolveu encetar a bandeira da cultura livre – pessoalmente, faço uma avaliação de que seria a sua base para a candidatura ao Senado, e ele perdeu. Não é possível limitar-se o processo de formação cultural e, portanto, as obras podem e devem ser colocadas na rede, de uma maneira ampla, porque assim se realiza o processo cultural de um povo. Entendo que nem tanto ao céu, nem tanto ao mar. Ainda que eu respeite a posição desse professor, com ela não concordo e nem poderia concordar, porque entendo que se trata de uma profunda inversão do que se pretende fazer, uma grande contradição do que a realidade apresenta a todos nós.

O que pretendo dizer com isso? A rede é por sua essência anárquica. Com isso, não estou me utilizando de uma metáfora para simplesmente criticar ou tentar reduzir algo que considero de suma importância na vida moderna. A rede veio para ficar, mas, se é anárquica, por hora não há controle sobre ela. Se não há controle, como crio uma *foundation*, chamada *creative commons*, e disponibilizo licenças eletrônicas na rede, em que aqueles que quiserem aderir aderem e, para cada modelito daquelas licenças, escolho o tipo de utilização que pretendo dar à minha obra?

Suponhamos que, por um motivo qualquer, entendo que a minha obra não pode sofrer nenhum processo de limitação. Pergunto-lhes: quem fará esse controle? Se uma das questões cruciais que a rede expõe para o universo jurídico é exatamente a ruptura da territorialidade, como obter decisões coercitivas, quando um contrato eletrônico foi assinado e descumprido? Isso me parece absolutamente inexequível, uma coisa morta. Desconfio que todo o escarcéu, toda a construção que se faz em torno desse sistema – quero dizer claramente que essa é uma reflexão que venho alimentando e estudando, mas com um certo equilíbrio, um certo bom senso –, cumprirá um outro desiderato, uma outra finalidade.

Quando estive na cidade de Santiago, no Chile, ouvi um debate entre Felipe González e José Saramago, o que foi um privilégio, primeiro porque Felipe González me surpreendeu. Na minha ignorância, desconhecia que ele era um homem sensível, inteligente, culto, embora conhecesse muito mais do escritor Saramago. Houve um momento em que o escritor disse abertamente para o público ouvir: "Eu me recuso a ser chamado de produtor de conteúdo. Não aceito que o que eu crie seja conteúdo. Eu crio obra". Confesso que registrei aquele desabafo, mas não alcancei, naquele momento e dois anos depois ainda, a verticalidade daquela reflexão, aonde ele queria chegar; qual seria a ferida em que estava colocando o dedo.

Como a questão gira em torno da dicotomia ideia e forma de expressão, peço licença para ler o art. 7º da lei de regência em matéria de autor, que estabelece a seguinte redação:

> São obras intelectuais protegidas as criações de espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro.

Vejam os senhores que esse artigo, que dá um referencial ou faz um elenco das obras conhecidas, que são objeto de criação, está em absoluta consonância com o que estou abordando aqui, relativamente a essa grande contradição entre ideia e forma de expressão.

Voltando à questão do Saramago, a "ficha só caiu" na minha cabeça no dia em que li a notícia de que o *Google* tinha comprado o *Youtube* por 1,65 bilhão de dólares. Confesso que o cenário se abriu diante dos meus olhos, porque me remeti à fala de Saramago e comecei a perceber o que subjaz a esse universo desconhecido. Não estou fazendo afirmações absolutas, estou pensando, refletindo, buscando na pluralidade a compreensão desse aspecto, mas é obvio que quem paga um 1,65 bilhão de dólares para ter um *site*, tem uma finalidade específica. Que *site* é esse? É um site que tem conteúdos áudio-visuais. Veio o segundo elemento da reflexão: para onde vai tudo isso? Para a plataforma da telefonia móvel.

Dá para perceber, sem rebuço, que essa linha está sendo traçada. E alguns dados estão aí para comprovar: as indústrias de provedores de acesso lucraram, nos Estados Unidos, 10,7 bilhões de dólares anuais, enquanto que a indústria de *copyright* só faturou 2,5 bilhões de dólares; diariamente, 65% de cerca de um bilhão e meio internautas usam pelo menos uma das ferramentas do *Google;* 40 bilhões de buscas por mês – claro que esse dado já está defasado; o *Google* fechou o ano de 2008 com um valor de 86 bilhões de dólares, o dobro da indústria musical mundial, que faturou 40 bilhões de dólares; o *Google* controla 69% do mercado de propaganda *on line* e recebe oitenta e oito *cents* de dólar por clique de patrocinadores.

Convenhamos que esses dados evidenciam, sem nenhuma dificuldade, que a luta que se trava é econômica. Quero fazer uma observação, relativamente ao Ministério da Cultura do nosso País que, neste momento, propõe mudar a lei autoral brasileira, uma lei que está em vigor há dez anos. Agora que toda a construção pretoriana se faz, no sentido de orientar e educar a sociedade brasileira, propõe-se uma alteração integral da lei, quando até defendo a sua modificação parcial nos aspectos que possam estar defasados. Não resta dúvida de que é uma lei moderna, em consonância com os principais estatutos da sociedade internacional, universal, europeia, mas se percebe que os segmentos de criação intelectual estão buscando ampliar o prazo de proteção, e o Ministério da Cultura de um Governo que se propõe a desenvolver uma melhoria de qualidade de vida para a sociedade brasileira não percebe ou, se percebe, silencia-se em torno da profunda contradição entre alimentar o proprietário da rede, que se chama *Google,* em detrimento do criador nacional. Essa é uma contradição, perdoem-me, que não consigo perceber.

De qualquer sorte, tem um lado positivo do Governo, na medida em que pretende elidir, eliminar, afastar a ignorância digital do brasileiro – estou em consonância com esse programa. Se o Presidente Lula deseja

salpicar de computadores o nosso chão, que o faça. Só que não pode fazê-lo à custa do trabalho de criação de terceiros. Esse me parece o momento mais grave que estamos vivendo.

Do ponto de vista dos casos que envolvem o direito de autor, as cortes brasileiras têm desempenhado um papel fundamental, porque, ainda que algumas decisões possam representar contradição ou inadequação na compreensão desse ou daquele fato, a jurisprudência nacional tem educado exemplarmente o respeito ao processo de criação do brasileiro.

Esses dados apresentados foram retirados do livro de Ken; ele próprio faz uma autocrítica em relação à rede. Não considero que trezentos anos de construção autoral deixaram de existir, a partir do surgimento de uma tecnologia da importância da internet. Não tenho nenhum fetiche em relação à internet. Entendo apenas e tão somente que a rede é um meio complexo, na medida em que nem tudo que cai na rede é passível de controle ou de compreensão.

Não fico perplexo diante dessas modificações. Ao contrário, vejo-as como uma decorrência natural de uma sociedade internacional que evolui e que se modifica. A fila anda e vai continuar andando. Quando se propõe a discussão das questões que envolvam o trânsito das obras nas infovias de conhecimento eletrônico, é preciso não perder de vista essa circunstância.

Agradou-me, extremamente, tomar conhecimento de uma decisão do Superior Tribunal de Justiça em que o *Google* foi condenado a pagar multa diária R$ 5 mil reais – em valor máximo limitado R$ 500 mil reais – por dia de veiculação, na internet, de comunidades vetadas judicialmente por ofensa a menores, moradores de três municípios do Estado: Pimenta Bueno, São Felipe d'Oeste e Primavera de Rondônia. Essa decisão foi confirmada, e o Ministro, em seu voto, afirmou que "a internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e sem responsabilidade pelos abusos que lá venham a

ocorrer". Segundo ele, "no mundo real, como no virtual, o valor da dignidade da pessoa humana é um só".

Essa compreensão e essa sensibilidade não só jurídica, mas, acima de tudo, moral para compreender que, em que pese as transformações que os meios eletrônicos propiciam, que as tecnologias ofertam, não é possível desrespeitar neste País. Estou à frente dessa luta com vários outros companheiros advogados militantes na área da propriedade intelectual, para se manter e preservar essa possibilidade, tanto mais numa sociedade como a nossa, que dá condições amplas ao direito de herança. Se o direito de herança é resguardado pela legislação brasileira, por que o autor não pode deixar para a sua descendência o fruto do seu labor intelectual? Ou por que ele, à sua revelia, deve ficar adstrito à cultura do remix, à cultura do recorta e cola, que empobrece o processo cultural?

Assusta-me afirmações de que a propriedade intelectual engessa o processo cultural brasileiro e de que a propriedade intelectual tem uma função social. Concordo que a função social da propriedade intelectual é proteger o autor, sem o qual não existe obra e sem obra não existe processo cultural. O que mais me impressiona é que subjaz a toda essa reflexão a questão mais grave: para aonde isso está indo? A quem isso beneficia? Quem financia, por exemplo, o c*reative commons, o Google*, o *Yahoo*? É muito dinheiro.

Para mim, que acompanho a questão da propriedade intelectual há alguns anos, é muito estranho, de repente, assistir emergir um movimento, que se reputa glorioso e definitivo, na medida em que vai possibilitar a todo criador ser conhecido no mundo e, ao mesmo tempo, ter condição de implementar a sua obra. Não tenho nada contra essa prática. Penso que aqueles que assim desejarem fazer, que o façam. Mas que não sejam iludidos, porque quem não faz sucesso no mundo real, dificilmente o fará no mundo virtual, já que esse apenas reproduz um dado de realidade. Não discuto que a internet oferece mais possibilidade

de o autor dar conhecimento à sua produção intelectual, o que não significa, necessariamente, que aquele que disponibilizou a sua ópera, a sua canção ou a sua partitura na rede se torne um Beethoven ou um Mozart, ou aquele que lançou um texto na rede se torne um Jorge Amado, um Graciliano Ramos ou um Fernando Pessoa.

Estava participando de uma conferência em Belo Horizonte, quando um jovem se levantou da plateia, indagando-me se eu o prenderia por baixar música da internet. Disse-lhe que não havia lido o programa, já que não sou delegado de polícia, mas apenas um modesto professor de Direito, que estava exercendo a liberdade de dizer o que pensa. Aprendi uma coisa e ensinei aos meus filhos: o que é dos outros a gente não pega. Seria ingenuidade de aquele rapaz supor que baixa música de graça da rede. Como baixa de graça? Como se acessa a rede? Não é pela telefonia móvel? Cada clique não são oitenta e oito *cents* de dólar para o *Google*? E a telefonia, o que leva?

Na verdade, alimentam-se grandes conglomerados internacionais, em detrimento do autor nacional. E é o direito de autor que é acusado de engessar o processo cultural do País. Pelo amor de Deus, penso que está na hora de mudar essa mentalidade e de acreditar que o meio eletrônico, como a internet, deve e pode ser utilizado da maneira que a pessoa desejar.

Mas vamos dizer para as pessoas mais jovens ou vamos entender que as coisas não ocorrem dessa maneira ingênua e que não subjazem em torno dessa grande questão interesses econômicos absolutamente vultosos e que, evidentemente, não estão em consonância com o direito dos criadores.

Muito obrigado.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

O Seminário de Direito Eletrônico é uma iniciativa do Centro de Estudos Superiores do Instituto dos Magistrados do Distrito Federal – IMAG/DF.

Iniciaremos a segunda palestra, que tem o tema "Contratos Eletrônicos". Para ministrá-la, convidamos o palestrante Dr. Marco Antônio Araújo Júnior.

O Dr. Marco Antônio Araújo Júnior possui graduação em Direito, pela Faculdades Integradas de Guarulhos e especialização em Direito das Novas Tecnologias, pela Universidade Complutense de Madrid, na Espanha.

Atualmente, é Diretor Pedagógico da Rede de Ensino Luiz Flávio Gomes. É, ainda, autor dos livros "Coleção Elementos do Direito - Ética Profissional", "Coleção Resumos de Bolso – Ética Profissional" e "Exames da OAB".

Lembramos que a participação é aberta. Caso alguém queira fazer uma pergunta, estenda a mão, e levaremos o microfone.

Com a palavra, o Dr. Marco Antônio Araújo Júnior.

PALESTRA VI: CONTRATOS ELETRÔNICOS

MARCO ANTÔNIO ARAÚJO JÚNIOR
Pós-Graduado em Derecho de
Las Neuvos Tecnologias – Universidad Complutense de Madrid

Muito obrigado.

Senhores, bom dia. É um prazer estar aqui. Agradeço ao Instituto dos Magistrados do Distrito Federal pelo convite e o parabenizo por esta iniciativa.

Falar sobre Direito Eletrônico é sempre muito bom. Trata-se de um tema novo, de dez anos para cá. Estamos caminhando, ainda, na formatação dessa nova área do Direito, que, para alguns, nem é, efetivamente, uma nova área do Direito, mas ouso dizer que é uma área que irá estudar o futuro do Direito. Portanto, estamos trabalhando com as informações do futuro do nosso Direito.

Foi-me proposto falar sobre Contratos Eletrônicos e aceitei de plano, porque é um tema bastante interessante, primeiro, pela ótica de analisar como está a questão contratual no plano digital; segundo, para falar um pouco da relação de consumo na internet, que creio ser um tema até um pouco mais palpitante do que a própria parte contratual.

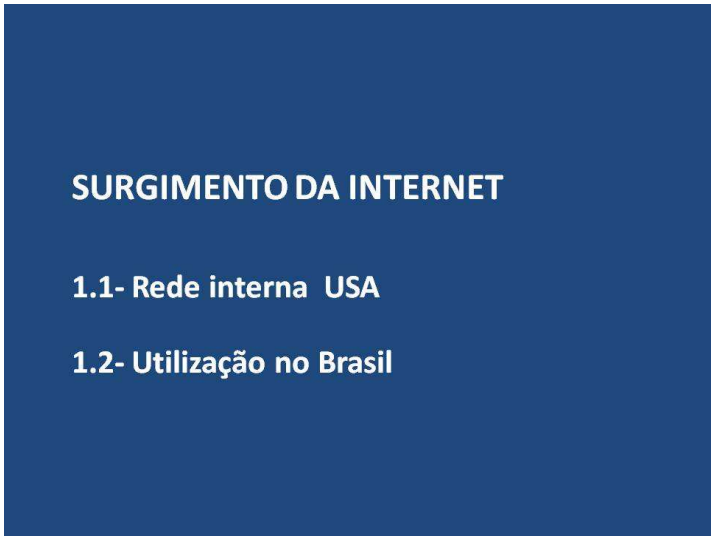
Quando se fala em contratos eletrônicos – já ouvi alguns doutrinadores falarem em contratos virtuais. Sempre me preocupa um pouco essa expressão virtual, que, às vezes, é empregada deforma incorreta, diria, pelo menos equivocada, porque o contrato não é virtual, o contrato é real, ele existe, apenas foi firmado em um ambiente virtual, e essa relação do virtual para o real aplica-se em várias questões que envolvem o Direito Eletrônico.

Podemos comparar com a questão do crime, que não é o meu tema, será tratado hoje com o Professor Rossini, um excelente Promotor de Justiça, que irá falar com os senhores depois do almoço. Da mesma forma que o contrato não é virtual, ele é real, o crime também não é virtual, o crime é real. O que mudou é que ele foi realizado no meio virtual.

A discussão é: o velho e antigo contrato, cujo principal princípio era o **pacta sunt servanda**, continua tendo valor se foi realizado no âmbito virtual? De que forma ele tem valor? Qual local é considerado o momento da efetivação do contrato? Como ficam aquelas características da eficácia e da vigência? Mais do que isso: como o Judiciário vem enfrentando essa questão do contrato eletrônico?

Na minha palestra, hoje, vou falar um pouco sobre esses temas, sem prejuízo de falar sobre o contrato de consumo eletrônico, talvez o contrato que mais façamos, atualmente, nas nossas vidas, e qual a garantia que tem o consumidor quando realiza um contrato dessa natureza.

Iniciarei fazendo duas considerações muito rápidas. Para falar sobre contrato eletrônico, tenho que falar um pouco como surgiu a internet, qual a sua finalidade e como se consolidou no Brasil.



A internet surgiu em 1969, nos Estados Unidos. Era uma rede de comunicação interna chamada de Advanced Research Projects Agency Network (ARPANet), que, na verdade, não surgiu com a finalidade de ser rede, mas com a finalidade de uma estratégia de guerra, efetivamente.

As informações ficavam em um local físico, único e, se, eventualmente, aquele local fosse bombardeado, perdia-se tudo. Por conta dessa manutenção de todas as informações em um local único, criou-se uma rede de comunicação entre os pontos de guerra para que pudessem repassar as informações de um ponto para outro, caso algum fosse bombardeado.

No final da década de 80 – surgiu na década de 60, em 1969, mais precisamente –, deu-se o início do uso comercial da internet nos Estados Unidos. Para nós, no Brasil, iniciou-se em 1992, mas, com a finalidade comercial somente em 1995 ou 1996.

De lá para cá, de todos os benefícios que a internet vem trazendo, penso que o ramo que mais tem sido chamado a trabalhar nesse tema é o Direito, porque os benefícios são muito grandes e o operador do Direito, seja ele advogado, seja ele juiz, seja ele promotor, enfim, em qualquer área que atuar, está sendo chamado a responder a esses conflitos que surgem na internet.

CRESCIMENTO DE USUÁRIOS POR CONTINENTE

Continente	População	Usuários 2000	Usuários 2009	% de Usuários 2009	Crescimento
Africa	991,002,342	4,514,400	67,371,700	6.8 %	1392,40%
Asia	3,808,070,503	114,304,000	738,257,230	19.4 %	545,90%
Europa	803,850,858	105,096,093	418,029,796	52.0 %	297,80%
Oriente Médio	202,687,005	3,284,800	57,425,046	28.3 %	1648,20%
América do Norte	340,831,831	108,096,800	252,908,000	74.2 %	134,00%
América Latina / Caribe	586,662,468	18,068,919	179,031,479	30.5 %	890,80%
Oceania / Australia	34,700,201	7,620,480	20,970,490	60.4 %	175,20%
TOTAL	6,767,805,208	360,985,492	1,733,993,741	25.6 %	380,30%

NOTES: (1) Internet Usage and World Population Statistics are for September 30, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2009, Miniwatts Marketing Group. All rights reserved worldwide.

Mostrarei um gráfico, apenas para curiosidade, sobre como está, atualmente, o crescimento na internet por continente. O gráfico foi retirado da *Internet World Stats*.

No slide ao lado, ressaltamos o Oriente Médio, pois foi o que teve o maior índice de crescimento: 1.648% de crescimento na utilização de usuários por continente.

CRESCIMENTO DE USUÁRIOS POR CONTINENTE

Continente	População	Usuários 2000	Usuários 2009	% de Usuários 2009	Crescimento
Africa	991,002,342	4,514,400	67,371,700	6.8 %	1392,40%
Asia	3,808,070,503	114,304,000	738,257,230	19.4 %	545,90%
Europa	803,850,858	105,096,093	418,029,796	52.0 %	297,80%
Oriente Médio	202,687,005	3,284,800	57,425,046	28.3 %	1648,20%
América do Norte	340,831,831	108,096,800	252,908,000	74.2 %	134,00%
América Latina / Caribe	586,662,468	18,068,919	179,031,479	30.5 %	890,80%
Oceania / Australia	34,700,201	7,620,480	20,970,490	60.4 %	175,20%
TOTAL	6,767,805,208	360,985,492	1,733,993,741	25.6 %	380,30%

NOTES: (1) Internet Usage and World Population Statistics are for September 30, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2009, Miniwatts Marketing Group. All rights reserved worldwide.

CRESCIMENTO DE USUÁRIOS POR CON

Continente	População	Usuários 2000	Usuários 2009	% de Usuários 2009	Crescimento
Africa	991,002,342	4,514,400	67,371,700	6.8 %	1392,40%
Asia	3,808,070,503	114,304,000	738,257,230	19.4 %	545,90%
Europa	803,850,858	105,096,093	418,029,796	52.0 %	297,80%
Oriente Médio	202,687,005	3,284,800	57,425,046	28.3 %	1648,20%
América do Norte	340,831,831	108,096,800	252,908,000	74.2 %	134,00%
América Latina / Caribe	586,662,468	18,068,919	179,031,479	30.5 %	890,80%
Oceania / Australia	34,700,201	7,620,480	20,970,490	60.4 %	175,20%
TOTAL	6,767,805,208	360,985,492	1,733,993,741	25.6 %	380,30%

NOTES: (1) Internet Usage and World Population Statistics are for September 30, 2009. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau . (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local Regulators and other reliable sources. (5) For definitions, disclaimer, and navigation help, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2009, Miniwatts Marketing Group. All rights reserved worldwide.

Nesse outro slide, ressaltamos a América Latina/Caribe que, em 2009, obteve um aumento de 30,5% no percentual de usuários e um crescimento de 890%. Não somos o que mais cresceu, mas também não somos o que menos cresceu.

Essa informação é somente para mostrar que, na verdade, se estamos discutindo o Direito Eletrônico no Brasil, essa discussão já é avançada em alguns países do mundo e começa a ser uma discussão solicitada em outros países, ou seja, sem dúvida nenhuma, estamos falando de uma nova área do Direito que está surgindo.

O gráfico ao lado mostra, em uma escala, quem mais cresceu. Podemos observar que o Oriente Médio cresceu mais e a América do Norte cresceu menos. Mas o

crescer pouco da América do Norte não significa que eles não estejam preparados; ao contrário, eles cresceram muito anteriormente e agora estão crescendo um pouco menos. Sobra para a África, para o Oriente Médio e para a América Latina um crescimento maior.

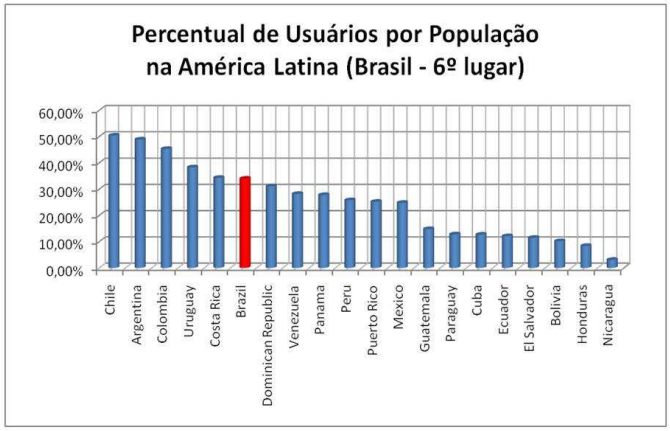
CRESCIMENTO DE USUÁRIOS NO BRASIL

País	População 2009	Usuários da Internet Atuais	% de Usuários 2009	Crescimento (2000-2009)
Argentina	40,913,584	20,000,000	48.9 %	700.0 %
Bolivia	9,775,246	1,000,000	10.2 %	733.3 %
Brasil	198,739,269	67,510,400	34.0 %	1,250.2 %
Chile	16,601,707	8,368,036	50.4 %	376.2 %
Colombia	43,677,372	19,792,718	45.3 %	2,154.3 %
Costa Rica	4,253,877	1,460,000	34.3 %	500.0 %
Cuba	11,451,652	1,450,000	12.7 %	2,316.7 %
Dominican Republic	9,650,054	3,000,000	31.1 %	5,354.5 %
Ecuador	14,573,101	1,759,472	12.1 %	877.5 %
El Salvador	7,185,218	826,000	11.5 %	1,965.0 %
Guatemala	13,276,517	1,960,000	14.8 %	2,915.4 %
Honduras	7,833,696	658,500	8.4 %	1,546.3 %
Mexico	111,211,789	27,600,000	24.8 %	917.5 %
Nicaragua	5,891,199	185,000	3.1 %	270.0 %
Panama	3,360,474	934,500	27.8 %	1,976.7 %
Paraguay	6,995,655	894,200	12.8 %	4,371.0 %
Peru	29,546,963	7,636,400	25.8 %	205.5 %
Puerto Rico	3,966,213	1,000,000	25.2 %	400.0 %
Uruguay	3,494,382	1,340,000	38.3 %	262.2 %
Venezuela	26,814,843	7,552,570	28.2 %	695.0 %
TOTAL	569,212,811	174,928,796	30.7 %	883.1 %

Fonte: E-Consulting Corp

Este gráfico mostra como está o índice de crescimento de usuários da internet no Brasil, pois apresenta a população de 2009, que é 198.739.269 milhões de habitantes, sendo 67.510.400 milhões de usuários da internet, o que equivale a 34% da população brasileira, um crescimento de 1.250%.

Chamo a atenção para o México, que tem uma população na casa dos cem milhões também e tem somente 24,8% de usuários da internet. Se formos comparar algo nesse gráfico, creio que a comparação tem que ser feita com o México.



Este outro gráfico mostra, em termos percentuais, a colocação do Brasil na América Latina. Considerando o percentual de usuários por população, o Brasil é o 6º colocado, conforme os dados de 2009, perdendo para o Chile, Argentina, Colômbia, Uruguai e Costa Rica.

Isso demonstra que, se, até hoje, não precisamos lidar muito com

essa questão da internet no campo jurídico, doravante teremos um problema sério, porque começará a ser uma cobrança cotidiana.

Não são estranhas decisões de magistrados que não conhecem o Direito Eletrônico e, mais ainda, não conhecem, efetivamente, a tecnologia que está disponível, o que nos preocupa, porque, se o magistrado não a conhece, a dificuldade em conhecê-la irá levá-lo a uma decisão muitas vezes equivocada ou errada.

Não é o tema aqui, mas não consigo deixar de tratar de uma decisão proferida no Mato Grosso do Sul, logo que surgiu uma discussão sobre *spam, que*, como os senhores já conhecem, é aquela mensagem indesejada que recebemos na nossa caixa de correio eletrônico. Essa expressão *spam* foi criada nos Estados Unidos. Na verdade, *spam* não tem nada a ver com *e-mail*, é uma marca de um presunto. Dizem as doutrinas que tratam do tema que esse presunto era servido como os amendoins, quando íamos ao restaurante e o garçom servia amendoins mesmo que não o tenhamos pedido. Nos Estados Unidos era servido o famoso *spam*, uma latinha de presunto, mesmo que não tivesse sido pedido.

A expressão *spam* acabou sendo o nome de uma prática muito costumeira no Brasil, que é a prática de mensagem indesejada, que gera problemas seriíssimos, inclusive de dano material, porque essa mensagem pode vir com vírus *trojans*, que pode ser autoexecutável na máquina, pois sem que tenhamos notado pode ter sido introjetado um programa espião e passamos a ser espionado por alguém que está, de forma remota, observando os seus dados, ou seja, você passa a ser personagem de um grande *big brother*, sem, contudo, concorrer a um milhão e meio no final. Aliás, o risco de perder um milhão e meio se você o tiver na conta é muito grande, porque pode ser furtado valor da conta corrente.

Entrei nessa questão do *spam* para dizer como a Justiça já se mostrou em relação a este assunto. Em uma decisão no Mato Grosso do Sul, uma Juíza que, à época, estava no Juizado Especial, considerou o *spam* uma mala direta eletrônica, portanto que a conduta do *spam* não

era uma prática comercial indevida.

Considero que, atualmente, o *spam* é uma prática comercial indevida, inclusive essa é a sua melhor definição. Aliás, foi uma definição solicitada, não foi recebida, mas foi fornecida em uma prova oral na magistratura do Estado de São Paulo, no Exame nº 181, em que houve o seguinte diálogo:

"Um Desembargador perguntou para o candidato: você tem *e-mail*, Doutor? Sim, Excelência, tenho *e-mail*. O senhor recebe mensagens que não pediu? Sim. Qual o nome dela? *Spam*. Qual a natureza jurídica dela? Complicado, Excelência, não há na Doutrina. Alguns falam. Gostaria que o senhor falasse."

Na verdade, um dos únicos a escrever sobre esse assunto havia sido o próprio desembargador que estava na banca. Portanto, estudar para passar em um concurso tem que estudar muito mais o que o desembargador pensa do que, efetivamente, o que está no edital, pois, na verdade, ele irá perguntar o que gosta e o que sabe.

Repito: considero que o spam é uma prática comercial indevida, abusiva, mas a Juíza considerou que não. A Juíza entendeu que o *spam* era uma mala direta eletrônica, que, salvo melhor juízo, não pode ser considerado.

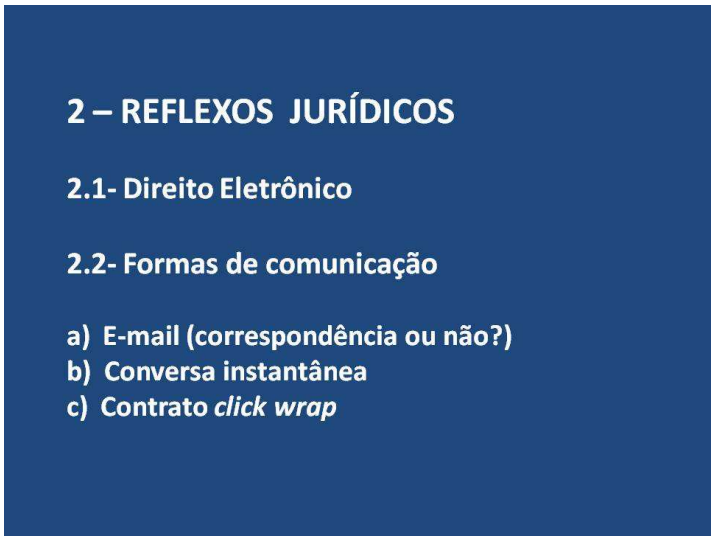
Senhores, vamos renovar o que é mala direta no nosso conceito, isso já é coisa do passado. Algumas coisas entregam a idade da pessoa, a mala direta é uma delas, pois falar mala direta já é coisa do passado, não se usa mais. Mala direta era aquela correspondência que o sujeito após consultar uma lista telefônica, imprimia dez mil folhetos do mesmo conteúdo naquela impressora matricial que tinha a etiquetinha, que também é coisa do passado, emitia diversas etiquetas, colava, ia ao Correio e postava, havia um preço especial, inclusive, e a mala direta chegava à sua casa. Quando abríamos a caixa de correio havia uma cartinha que não sabíamos, efetivamente, de onde era; se quiséssemos

líamos ou rasgávamos. O custo da mala direta é cem por cento do remetente, quem remete é quem paga. Ele paga o papel, paga a etiqueta, paga o selo, paga tudo.

O *spam* não é uma mala direta, pois o seu custo é dividido com quem recebe, porque existe a internet que pode ser paga, com um limite de dados para receber e porque pode causar um problema no *hardware* do computador. Então, quem recebe um *spam* também paga por ele. Não é possível dizer que é mala direta, a não ser que pensássemos que essa mala direita fosse cem por cento por conta de quem a encaminha, o que não é verdade.

Costumo brincar dizendo o seguinte: afirmar que o spam é uma mala direta eletrônica é a mesma coisa que admitir, como correta, a prática de um sujeito, de madrugada, ligar para o nosso telefone celular a cobrar. Ao atendermos a ligação, pensamos que aconteceu algo desagradável. E o sujeito pergunta se está tudo bem e diz que está vendendo seguro de casa, de carro e outros, ao que respondemos: amigo, você me liga de madrugada, a cobrar, para vender seguro? Desculpe-me, mas essa prática é abusiva. É o *spam*: a pessoa vende um produto seu e o encaminha para outros a fim de tenham o custo do spam, uma prática, absolutamente, abusiva.

A partir do próprio *spam*, surge a vinculação da oferta, por exemplo, porque, às vezes, o produto não interessa e, outras vezes, pode interessar. O *spam* já é a fase pré-contratual, porque traz a oferta para o consumidor. Trabalhar o *spam* significa trabalhar uma fase pré-contratual que tem previsão, inclusive, no Código de Defesa do Consumidor.



Apresento algumas formas de comunicação. A primeira delas é o *e-mail*. Há uma discussão sobre o *e-mail* ser uma correspondência ou não – creio que o Roni deve ter falado sobre o tema ontem, porque é um dos defensores dessa distinção. Qual a importância em saber se o *e-mail* é correspondência ou não? Importância constitucional praticamente. Se o *e-mail* for considerado correspondência, tem garantia de inviolabilidade; se não for considerado como tal, não é inviolável.

Levanto essa dúvida porque existe uma lei específica, Lei nº 6.538/1978, bastante antiga, que apresenta o rol do que é correspondência: a carta, o telegrama, o telex – que já está no passado –, mas não cita *e-mail*, porque não existia àquela época.

Posso acrescentar o *e-mail* nessa lei? A doutrina divide-se. Parte da doutrina entende que *e-mail* é correspondência, portanto já garante a inviolabilidade do *e-mail*. Outra parte entende que o *e-mail* não é correspondência, porque sustenta que este não tem a característica do sigilo, e a correspondência tem intrínseca essa característica. Podemos perguntar: como o *e-mail* não tem a característica do sigilo?

Vamos fazer um exercício rápido: Uma carta dobrada, colocada dentro de um envelope colado, possui a característica do sigilo. Se alguém a abrir, pratica o crime de quebra da inviolabilidade.

No passado, tínhamos acesso a várias formas de quebra de sigilo na carta, uma delas era o 'bule da vovó', ou seja, o sujeito colocava a carta no bule da vovó, a cola ia soltando e, assim, conseguia abri-la. Isso é, teoricamente, uma infração.

O *e-mail* não nenhum sigilo garantido, pois é um pacote de dados que encaminho do meu computador para o computador de outra pessoa. Nesse meio tempo, alguém pode absorver esse pacote de dados. Se houver um *hacker*, ele pode, tranquilamente, invadir o pacote de dados, colher as informações e tê-las em mão. A rigor, mando meu e-mail para meu servidor, que distribui os dados na nuvem, que desce para o seu servidor e que envia para o seu computador. A rigor, não há sigilo nesse procedimento. Mas, se o *e-mail* for criptografado, estarei dificultando o acesso ao pacote de dados.

Quero lembrar que a criptografia, em uma forma básica – sem avançar nesse detalhe, porque seria um motivo para uma exposição única, assinatura digital –, é um conjunto de códigos que coloco no meu documento e que a outra pessoa só vai recebê-lo e identificá-lo se ela também tiver os mesmos códigos.

Ao criptografar o meu *e-mail*, a lógica das palavras se desfaz e transforma-se em códigos. Se a pessoa do outro lado não tiver a chave para a abertura daquele código, não conseguirá entender a mensagem. Até pode recebê-la, mas não conseguirá entendê-la.

Há discussão sobre um sistema seguro de criptografia. Há quem diga que a criptografia nada mais é do que aquela brincadeira de criança que se chamava "língua do P". As pessoas brincavam de colocar um P antes de cada sílaba. Vencia a brincadeira quem conseguia falar. Se duas pessoas falavam na "língua do P" perto de uma terceira que não tinha esse conhecimento, a terceira pessoa ficava sem saber o que estava acontecendo. Quando descobria que era a "língua do P", matava a charada, quebrava a criptografia. Se a criptografia não tiver a segurança necessária para fechar o documento, o *e-mail* continuará sendo uma correspondência aberta.

Trouxe duas teses sobre a questão de o e-mail ser correspondência ou não. Existem os que sustentam que é e os que sustentam que não. Cada um dos senhores pode adotar uma das teses. Na minha opinião, o *e-*

mail é correspondência. Não partilho da tese de que, embora seja aberto, não seja correspondência. É uma evolução do documento carta que passou para o campo digital.

Outra forma de manifestação de comunicação na Internet é a conversa instantânea. Temos muitos exemplos de conversas instantâneas pelos sites de relacionamento, pelo famoso MSN.

A terceira forma de comunicação é muito interessante e, para alguns doutrinadores, é considerada uma forma de contrato, qual seja, o *click wrap*. Posso garantir que todos os senhores já fizeram esse contrato.

Todos têm *e-mail*. Quando se entra em um servidor de *e-mail* pessoal – que não seja corporativo, porque se trata de uma outra característica –, certamente tem que dar um 'aceite' às regras de funcionamento daquele sistema. Aquele é um serviço que está sendo colocado à sua disposição, oneroso ou não, não importa nesse instante, mas tem que se dar um 'aceite' àquela regra.

Funciona assim: se dissermos que não aceitamos, não iremos brincar; mais do que isso, se aceitarmos parcialmente, também não brincaremos; temos que aceitar tudo. Por vezes, o contrato *click wrap* vem já com a bolinha no 'aceite', que é para não termos tempo para pensar. Quantos dos senhores leram os termos do contrato integralmente? Ninguém lê. Eu olho para o contrato e penso: para que vou ler se não vou conseguir mudar? Ler só para me irritar?

É lógico que se trata de um contrato de adesão, quer sob a ótica do Código Civil brasileiro quer sob a ótica do Código de Defesa do Consumidor, mas é uma prática que impossibilita discussão. Teremos tem que entrar e depois, se causar problema, iremos discutir judicialmente.

O contrato *wrap* é muito comum para *softwares*, para serviços. Quando se faz o *download*, aparecem as cláusulas do contrato e, ao final, existem duas possibilidades: aceita e não aceita.

As regras de boa conduta, sob a ótica do Código de Defesa do

Consumidor, indicam aos fornecedores que não coloquem a bolinha em lugar nenhum, que deixe pelo menos para que o usuário a coloque, como se esse ato representasse uma manifestação de vontade, não uma indução da manifestação. Mas não muda nada. Se a bolinha não vier no 'aceito', e clicarmos no 'aceito', mas quisermos discutir o contrato de adesão depois, seja bem-vindo ao Poder Judiciário. Não muda absolutamente nada. É somente uma regra de boa conduta.

Para falar de contrato eletrônico, temos que mencionar algo que não para de crescer em nosso País – aliás, que não para de crescer no mundo – que é o comércio eletrônico, o chamado *e-commerce*.

O que é o comércio eletrônico? Lanço um conceito que foi tirado de parte de cada doutrina. Comércio eletrônico é toda relação jurídica onerosa que se estabelece entre um fornecedor, de produto ou de serviço, e um consumidor, por intermédio da rede de computadores. Considero que só é comércio eletrônico efetivamente se for oneroso. Sobre essa onerosidade falaremos um pouco quando estudarmos a relação do Código de Defesa do Consumidor.

O CDC, no art. 3º, § 2º, dispõe que, para ser serviço, estar sujeito à aplicação do CDC, tem que ser qualquer atividade colocada no mercado de consumo, mediante remuneração. Sabemos que essa remuneração de que trata a lei pode ser direta ou indireta. Então, até mesmo quando o serviço não foi efetivamente pago, mas quando há uma remuneração indireta, encaixa-se no conceito de *e-commerce*. É oneroso sob a ótica da remuneração direta ou indireta. Traduzindo em miúdos: mesmo um serviço que é colocado à disposição de forma gratuita, é considerado

serviço para o Código de Defesa do Consumidor.

Comentávamos, antes de entrarmos, que um dos serviços mais importantes para a população do nosso século – penso até que seja possível dividir antes e depois desse serviço – é o *Google*. O que não está no *Google* não está no mundo. Quando temos dúvida sobre algo ou alguém ou um endereço, basta pesquisar no *Google*. Ficamos reféns de um serviço que é privado, que nos é prestado de forma gratuita – lógico que não absolutamente gratuita. É serviço porque a remuneração do *Google* é indireta, nenhum de nós paga pelo *Google*, mas, se quisermos anunciar alguma coisa nesse *site*, temos que pagar e, por conta do acesso do consumidor, vários fornecedores anunciam a preço de ouro, e ai de nós se nos indispusermos com o *Google*. A BMW vivenciou uma experiência há uns cinco anos e encarou uma gigantesca demanda judicial. O *Google* teve um desentendimento com a BMW, num determinado momento, por conta de quotas comerciais e resolveu, após ter conhecimento de que a BMW não iria mais fazer o anúncio com eles, que toda vez que alguém digitasse BMW, indicaria o *site* da Ferrari. Perceberam que o *Google* é capaz de acabar com a vida da pessoa ou de alavancar qualquer outro tipo de negócio. Na verdade, ele detém uma informação de forma privada que leva a resultados positivos ou catastróficos.

Atualmente, discute-se – falávamos disso no III Congresso Internacional de Direito Eletrônico, no ano passado, que aconteceu em Maringá, e o IV Congresso este ano acontecerá em Curitiba - o direito ao esquecimento, pois o *Google* tem uma ficha corrida mais importante que a ficha da polícia. Se uma pessoa praticar um crime, for condenado por ele, cumprir a pena e reabilitar-se, e alguém tirar uma certidão negativa do seu nome, não aparecerá nada; em compensação, se pesquisar no *Google*, aparecerá que há trinta anos alguém praticou um crime, aparecerá a página do jornal, se tiver foto, também aparecerá, ou seja, o *Google* tem um poder maior do que o próprio Estado na solução dessa informação. É uma manipulação de informação muito perigosa.

Enfrentamos uma guerra entre a China e o *Google* bastante séria nesse sentido.

Então, falando sobre o direito ao esquecimento, o *Google* não tem o direito de informar o que já passou. Um médico ajuizou uma ação contra o *Google*, porque no passado ele foi condenado por lesão corporal gravíssima e a informação não saía da página. Estamos falando de uma prestação de serviço altamente moderna que, se analisada sob a ótica do Direito, pode ser extremamente prejudicial, pode ferir a democracia.

Pois bem, tenho quatro tipos de participantes em uma relação de *e-commerce*, comércio eletrônico, e cada um deles tem uma nomenclatura interessante.

A primeira relação é B2B (*business to business*), negócio a negócio; são empresas que negociam entre si. De um lado, tenho uma empresa que fornece o produto e, de outro, um supermercado. Entre elas, há um sistema, e, na medida em que o consumidor passa no caixa do supermercado com aquele produto, automaticamente, baixa o estoque e também há uma solicitação do fornecedor.

A segunda relação é B2C – *business to consumer*, negócio a cliente. Nesse caso, cito um exemplo de algo que todos nós já fizemos ou quem não o fez ainda o fará um dia: é a relação de lojas virtuais, a compra pela internet. Há pessoas que afirmam que não fazem, em absoluto, compras pela internet e que nunca vão fazer, mas, em alguns casos, se não o fizer, não terão o produto. Um exemplo típico disso aconteceu com o show da Madona. Se não fosse a atuação do Poder Judiciário, o ingresso do show da Madona teria sido vendido no primeiro mês somente pela internet, não havia venda física. Então, se você não

quisesse comprar pela internet, não teria a possibilidade de adquirir o ingresso. A partir de uma provocação do Judiciário, concedeu-se uma liminar, dizendo que tal fato feria o poder de igualdade de contratações, mas a prática foi colocada. Daqui a pouco, haverá produto que é vendido apenas pela internet. Então, o B2C é negócio de um lado, consumidor do outro, compras pela internet. Uso o termo internet, mas pode ser celular; atualmente, mais do que isso, produtos são vendidos até dentro de um elevador. Existem prédios grandes, que se demora, pelo menos, cinco ou dez minutos para se deslocar do térreo ao último andar, composto de terminais de venda dentro dos elevadores. Às vezes, esse é o único momento que a pessoa tem para comprar alguma coisa e, então, ela digita a senha, o CPF, o código do cartão e realiza a compra. Segundo informações, a *Dell* é uma empresa que não tem loja; portanto, as vendas são 100% pela internet, B2C.

A terceira relação é B2G – *business to government*, o negócio do governo. Nesse caso, cito um exemplo: a negociação do fornecedor com o governo em um leilão virtual. Esse tipo de negociação está acontecendo cada vez mais, trata-se do leilão eletrônico.

E o último modelo é o C2C – *consumer to consumer*, do consumidor para o consumidor. Às vezes, a relação é só entre consumidores e, aí, a expressão consumidor não fica muito adequada, porque para ser considerado consumidor tem que ter, pelo menos, um fornecedor. Não existe uma relação de consumo em que só haja consumidor. Então, consumidor com consumidor fica uma questão estranha, mas a doutrina chama dessa forma. Eu diria relação entre os particulares. O melhor exemplo, de uma relação de *e-commerce* entre os particulares é o leilão virtual. Fazemos um anúncio de um computador, outra pessoa o *site* de leilão, oferece um valor de lance, e a venda é feita. Portanto, estabeleceu-se uma relação de pessoa física/pessoa física, pessoa jurídica/pessoa jurídica, uma forma de pessoa a pessoa, não de consumidor/consumidor, porque essa não é uma relação de consumo.

Algumas pessoas perguntam se essa relação que existe de pessoa/ pessoa nos *sites* de leilão seria considerada uma relação de consumo. Respondo que não com a outra pessoa que comprei, mas com o *site* sim. A internet é um mundo livre, podemos citar nomes, até porque estamos discutindo, academicamente, aqui dentro, então, vamos citar como exemplo o *site* www.mercadolivre.com.br, que é um dos maiores *sites* de leilão atualmente. Vamos imaginar que anunciei o meu computador para venda, alguém o comprou em um *site* de leilão, pagou o valor e eu não o entreguei. Nesse exemplo, o *site* de relacionamento agiu como mero intermediador do negócio, não chamou para si a responsabilidade do pagamento. O próprio *site* www.mercadolivre.com.br tem um outro tipo de serviço, que é o mercado pago. Nesse caso, a pessoa paga para o mercado livre, que só vai repassar o valor se, efetivamente, houver a entrega da mercadoria, o que é uma garantia. Não vou tratar desse exemplo, pois me parece claro, que, nesse caso, aplica-se o CDC.

Vamos tratar de um outro exemplo mais comum. Anunciei o meu computador à venda, alguém o comprou pelo valor que pedi e fez o depósito na minha conta. O acesso aos meus dados pessoais só é permitido após a oferta do lance. Assim, o comprador ficou sabendo qual é a minha identificação no *site*, mas não sabe onde moro, nem o meu nome correto. Após receber o dinheiro, não entrego o computador, uma situação que acontece muito. Nessa relação, aplica-se o Código de Defesa do Consumidor? Trata-se de uma questão tormentosa.

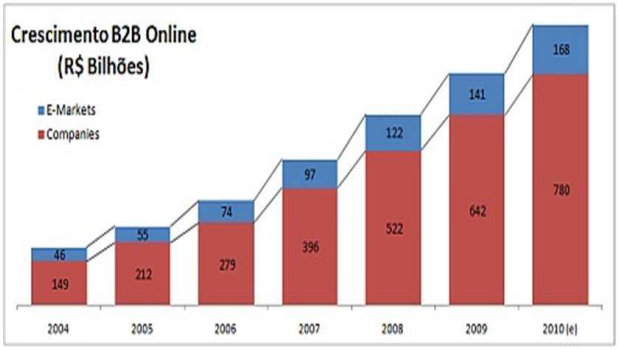
Vou dar a minha opinião e, depois, vou até trazer um julgado no mesmo sentido, mas já adianto que tem decisão para todo gosto. A minha opinião é que, quando esse *site* propõe-se a fazer a aproximação das pessoa – isso é um serviço – e a venda efetiva-se, ele ganha por isso. Então, além de ser um serviço, é um serviço oneroso, como consta no art. 3º, § 2º do CDC. Se a aproximação das pessoas caracteriza a prestação de um serviço, essa aproximação não pode ocorrer só na fase pré-contratual, tem que ser até a efetiva contratação, até a execução da

venda, e se não houver a entrega do produto – desculpa - o serviço proposto não foi feito de forma segura, portanto a responsabilidade pelo fato dos serviços é do Código de Defesa do Consumidor. Na minha opinião, o *site*, que faz o intermédio entre duas pessoas para a venda, é responsável caso ocorra alguma questão de vício ou de fato na relação de consumo.

Adiantando, esclareço que o Judiciário não vem pensando dessa maneira. Diversas decisões indicam que a atividade desse site é de mero aproximador, como seria – aí a decisão até cita – um classificado de jornal, por exemplo, em que alguém anuncia, uma pessoa interessa em comprar entra em contato com o vendedor e faz a compra. Não consigo entender dessa forma, porque no anúncio feito no *site* não se sabe quem é o vendedor, o que só é possível descobrir, efetivamente, depois da oferta do lance e do aceite do valor. Portanto, se não se sabe quem é o vendedor e quem segurou a essa informação foi o *site* que faz a intermediação, então, ele participou dessa relação.

Em um classificado de jornal, observamos que alguém está vendendo um computador, ligamos para confirmar e perguntamos como é o computador, qual o seu tempo de uso, porque está sendo vendido, pedimos o endereço da pessoa que está vendendo e vamos até o local para verificar o produto e, assim, caso tenhamos ficado satisfeito, efetivamos a compra. Se após dois, três ou quatro dias surgir um vício no computador, aí iremos demandar somente contra o vendedor, e não contra o jornal que o anunciou, evidente. Porém, essa não é a relação do *site* de leilão, que segura a informação, repassando-a somente depois do negócio feito, e cobra por isso não como cobra o jornal pelo anúncio, mas cobra um percentual de venda sobre o valor. Não é possível imaginar de outra forma, senão dizer que esses *sites* têm responsabilidade, sim, quando fazem intermediação entre duas pessoas.

VENDAS B2B – EMPRESA PARA EMPRESA EM 2009

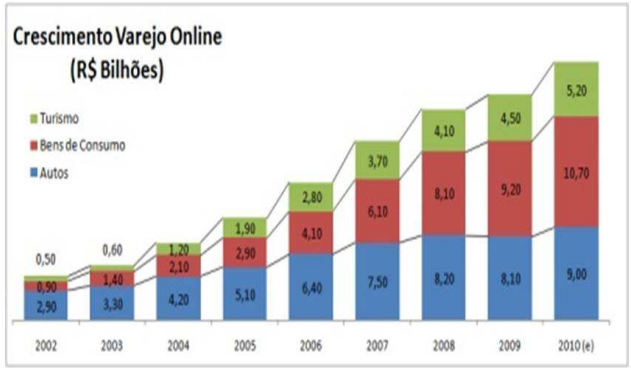


Fonte: E-Consulting Corp

Apresento-lhes dois gráficos sobre a evolução do varejo, apenas para mostrar como cresce o varejo *on-line* no comércio eletrônico. No primeiro gráfico uma análise do B2B e no segundo do BTC.

Nesse segundo gráfico, a cor verde representa a área do turismo, cada vez mais se compra pacote de turismo pela internet. Bens de consumo estão representados pela cor vermelha e, pasmem, automóveis, pela cor azul, o que significa que compramos carros pela internet. Essas informações são do *E-Consult Corp*.

EVOLUÇÃO VAREJO ON-LINE



Fonte: E-Consulting Corp

4 – CONTRATO ELETRÔNICO

4.1 – Contrato em geral

a) existência

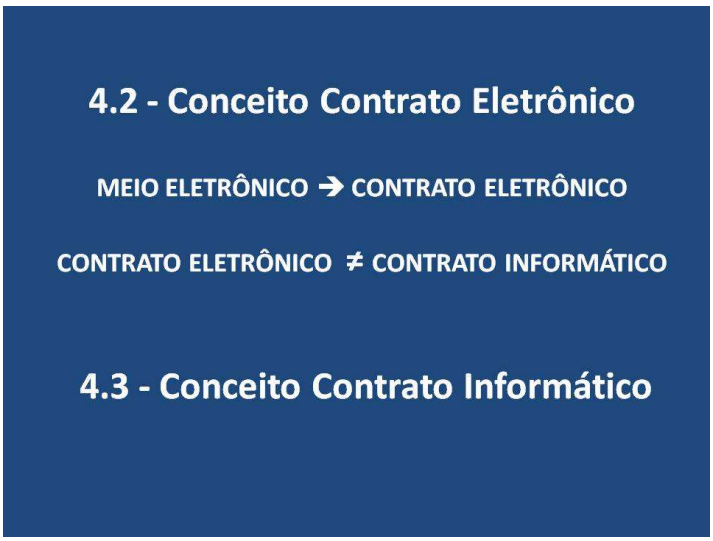
b) validade

c) eficácia

Falaremos, agora, sobre o contrato em geral que tem três requisitos que se aplicam também ao contrato eletrônico. O primeiro requisito é a existência. Para que exista um contrato tem que haver sujeito e objeto – são os dois fatos principais da característica do requisito da existência. Tem que haver declaração de vontade entre as partes. Os sujeitos e o objeto do contrato tem que ter ligação. Não existe contrato se não existir sujeito e objeto.

O segundo requisito é o da validade, que aprendemos há muito tempo. O sujeito tem que ser capaz, o objeto deve ser lícito e a forma não pode ser proibida em lei, pode estar prescrita ou não proibida em lei. Então, os três elementos da validade são fundamentais para que esse contrato eletrônico também exista. Importante: Se faltar um dos elementos o contrato existe; não significa que ele vai deixar de existir, mas pode ser nulo ou anulável, dependendo do elemento.

O terceiro requisito é a eficácia: não existe contrato se ele não produzir efeito dentro daquilo que foi combinado. O mandatário, por exemplo, se não tem poderes para realizar determinado ato e os realiza, não surtiu o efeito que se espera do mandato.



O que é o contrato eletrônico? Apresentarei, aqui, alguns conceitos.

O primeiro deles é de *Olivier Et Noir*, doutrinador francês, que escreve sobre o direito à internet e fala o seguinte: "O contrato eletrônico é o encontro de uma oferta de bens ou serviços que se exprime de modo audiovisual, através de uma rede internacional de telecomunicações e de uma aceitação sucessível de manifestar-se por meio da interatividade." Então, para *Olivier Et Noir*, contrato é aquilo que tem manifestação e interatividade. Essa segunda expressão fica gravada: interatividade. Se não tiver interatividade, não é possível considerar.

Semy Glanz, Desembargador do Tribunal de Justiça do Rio de Janeiro, autor de um livro muito interessante chamado "A Família Mutante", que aconselho a leitura, pois é um livro bastante legal, diz o seguinte: "Contrato eletrônico é aquele celebrado por meio de programas de computador ou de aparelhos com tais programas, que dispensam

assinaturas ou exigem assinaturas codificadas ou senha.” Quer dizer, contrato eletrônico não é somente feito na internet, pode ser feito por outro meio, como pelo celular. Nem sempre o contrato eletrônico tem assinatura codificada ou senha. Às vezes, ele não tem assinatura codificada ou senha e é contrato eletrônico.

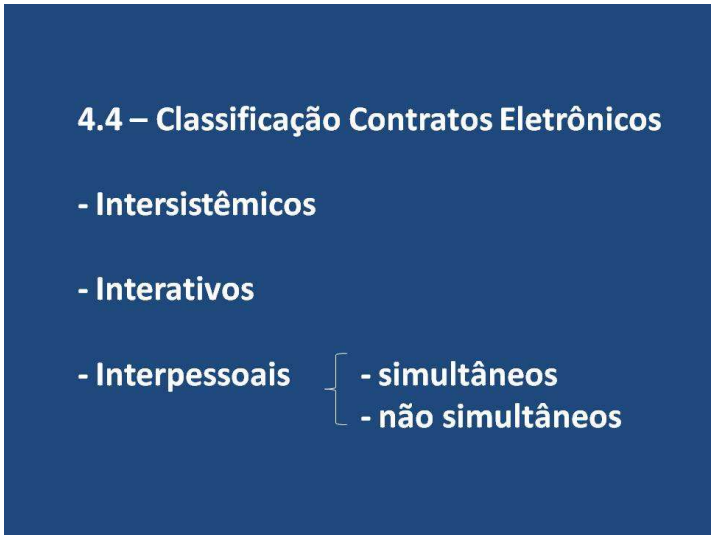
Apresento outro conceito que é um pouco a mistura do que os doutrinadores falam.

Contrato eletrônico é aquele em que o computador é um meio utilizado para manifestação das partes – o computador ou qualquer outro meio eletrônico – é o contrato realizado por meio eletrônico: internet, celular, enfim, elevador, que também é um programa de computador. Para que esse contrato seja válido, ele tem que ter um aceite, eletronicamente, consentido. Não sei se tem senha ou não, pois nem sempre precisa. Não sei se precisa ser criptografado ou não, pois nem sempre precisa. Agora, observem. Meio eletrônico é diferente de contrato eletrônico. Meio eletrônico é o local em que se realiza o contrato, e o contrato é especificamente a forma. Então, em qualquer meio eletrônico, faço um contrato eletrônico.

Trouxe uma diferença a respeito do contrato informático para que não haja nenhum tipo de confusão. Não gosto muito da expressão “direito da informática” ou “direito da internet” que alguns autores utilizam. Penso não ser muito correta essas expressões, embora um dos autores que a utiliza seja o Desembargador Federal Newton de Lucca, do TRF da 3ª Região, de São Paulo, por quem tenho uma admiração muito especial e talvez tenha sido o grande precursor do Direito Eletrônico no Brasil. Autor de excelentes obras sobre esse assunto. A expressão “direito da internet”, não me parece adequada, porque a internet é apenas um meio de comunicação. Evidentemente, representa uma revolução social, mas é apenas um meio de comunicação, e, a pensar que deveria existir o “direito da internet”, então qualquer outro meio de comunicação mereceria um direito.

Imaginem, há dez anos, o "direito do fax", que foi um avanço. Quando surgiu, as pessoas não acreditavam, falavam que não era possível que se passasse um documento de um lado e ele aparece do outro. Depois, perceberam que era perfeitamente possível, mas não existia o "direito do fax".

Outro avanço tecnológico foi o bip. Era algo impressionante. Conseguia-se localizar uma pessoa onde ela estivesse com aquele código. Hoje, se alguém usar um bip, dirão que ele é antigo mesmo. O bip foi substituído pelo celular, que, atualmente, é a coisa mais impressionante do mundo. Os senhores já se imaginaram sem celular durante alguns dias? Algumas pessoas têm crise, começam a passar mal, voltam na metade do caminho para casa porque esquecerem o celular. Outras, se não recebem ligação, ficam olhando o tempo todo para o aparelho. O celular virou uma febre em nossa vida. E quanto mais recursos ele oferecer, além de falar, melhor! Existe celular que tira foto, mede a temperatura, faz coisas absurdas! Existem algumas pessoas, atualmente, que já possuem dois aparelhos de telefone celular. Mede-se o *status* de importância da pessoa pela quantidade de aparelhos celulares que ela tem. Aquele que possui dois aparelhos é considerado uma pessoa muito importante. Quem tem apenas um, não é tão importante assim. Ainda assim, esse processo de evolução não mereceria o "direito do celular", por isso entendo que as expressões "direito da informática" ou "direito da internet" não são corretas.



O contrato informático, que é voltado para o ambiente virtual, não tem nada a ver com o contrato eletrônico. Por exemplo, um contrato de fornecimento de um *software* é um contrato informático.

Um contrato de desenvolvimento de um *website*, isso sim, é um contrato eletrônico. Essa é a diferença entre o eletrônico e o informático. Um contrato de compra e venda de um domínio é um contrato, efetivamente, informático.

Essa classificação ao lado é adotada pela doutrina majoritária que cuida de "Direito Eletrônico", em especial de contratos eletrônicos. É uma classificação muito interessante que começa a ser utilizada pelo Poder Judiciário. Veremos uma decisão do Tribunal de Justiça do Rio Grande do Sul, se não me falha a memória, que faz referência a essa classificação. Os contratos eletrônicos são divididos em três tipos: contratos intersistêmicos, contratos interativos e contratos interpessoais.

Contratos intersistêmicos – a classificação já diz – é um sistema com outro sistema. É aquilo que se chama de desumanização do contrato, porque não precisamos de ninguém para realizá-lo. É um contrato de rede fechada em que os sistemas aplicativos são previamente agendados para trabalhar. Vou repetir um exemplo: imaginem um supermercado que tem um sistema de estoque o qual se comunica com o sistema do fornecedor. À medida que o estoque vai baixando, o fornecedor recebe uma chamada no seu sistema, que já faz um pedido automático e determina a entrega para o supermercado. Não precisa de funcionário para fazer o pedido. Desumaniza, absolutamente, o contrato. Nesse tipo de contrato, um sistema está preparado para lidar com outro sistema e a comunicação é imediata.

O segundo tipo de contrato é chamado de contratos interativos, em que a relação é de pessoa x sistema, a pessoa interage com o sistema previamente agendado. Por exemplo, uma loja virtual, em que não há funcionário. Navega-se pela loja, faz-se o pedido, postula-se o desconto no caso de participação em algum programa de promoção, digita-se o código do desconto, o valor automaticamente é atualizado, digita-se o cep da residência, o frete é contabilizado, fecha-se o pedido, digita-se o número do cartão de crédito, espera-se um ou dois dias, e o produto

chega em casa. Nesse caso, há uma interação entre a pessoa e um sistema.

Em regra, como não há interação pessoa x pessoa, a pessoa é o sistema, os contratos interativos são de adesão, porque já está preparado o sistema e a pessoa adere ou não àquela cláusula, àquele processo, àquele produto. Tanto o Código Civil quanto o Código de Defesa do Consumidor têm praticamente a mesma característica em relação ao contrato de adesão. O Código Civil diz que o contrato de adesão é possível e será analisado da maneira mais favorável ao aderente, quando houver algum problema. O mesmo diz o Código de Defesa do Consumidor, com um pouco mais de rigor, porque, se a cláusula for considerada nula, pode o juiz, de ofício, declarar a nulidade. Então, no CDC ele também é analisada sob a ótica do vulnerável, que é o consumidor, e, de ofício, o juiz pode declarar a cláusula nula sem entender que ela é abusiva, se estiver no rol do art. 51 do CDC.

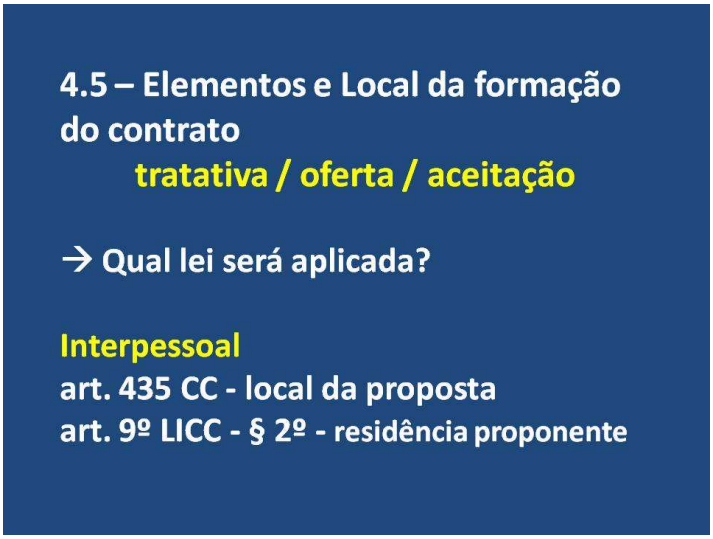
A terceira modalidade de contrato que trago para análise diz respeito aos contratos interpessoais. Como o próprio nome sugere, interpessoais são pessoas de um lado e do outro. São contratos em que as pessoas comunicam-se. Existem duas classificações: os interpessoais não simultâneos e os interpessoais simultâneos.

Interpessoais não simultâneos são aqueles realizados por *e-mail*. As características do ato jurídico são enviadas, e a outra pessoa que recebe o *e-mail* responde. Quero alertar que parte da doutrina entende que é simultâneo, mas penso que não seja, porque não há interatividade, não é imediato. A mensagem é encaminhada para uma caixa de correio, podendo ser respondida no mesmo dia ou após dois dias, ou até pode-se perder o prazo se o remetente, ao encaminhar, fizer a seguinte proposta: o valor é R$ 1.000,00 (mil reais) pelo prazo de três dias. Se deixar passar o prazo, perde-se. Então, não é simultâneo.

Existe o contrato interpessoal simultâneo. Pode-se contratar por intermédio de uma videoconferência, fixando as regras de contrato, o que

é muito comum, e aceitando os seus termos. Também é possível fazer uma contratação por celular – ela é instantânea, simultânea. Nesse caso, existe um exemplo interessante da doutrina, com a qual também não concordo, mas falarei a respeito.

A doutrina entende – refiro-me ao Prof. Ricardo Lorenzoni – que, por exemplo, quem tem tv por assinatura, pode acessar o *pay per view*, digitar uma senha, e imediatamente passará a ser assinante. Não é preciso ligar para mais ninguém, nem falar com funcionário, apenas digitar uma senha e passará a funcionar automaticamente. O Prof. Ricardo entende que o contrato *pay per view* tem características de um contrato interpessoal simultâneo. Eu acredito que não. Na minha opinião, não se trata de um contrato interpessoal, e sim interativo, pessoa x sistema. Não há ninguém do outro lado aguardando a senha chegar pela televisão, trata-se de um sistema que está preparado para receber aquela senha.



Este slide apresenta os elementos e o local da formação do contrato. Existem três características que são elementos da formação do contrato comum: as tratativas, a fase pré-contratual, a oferta e a aceitação, efetivação do contrato. Quando se fala das tratativas, verifica-se o estudo das possibilidades do contrato na fase pré-contratual. Quanto à oferta, se se tratar de um contrato de consumo, especialmente vale a pena chamar atenção para esta característica, porque, no contrato de consumo, a oferta vincula o fornecedor. Se houver uma oferta, ela terá que ser efetivamente cumprida, desde que respeitado um dos princípios mais importantes do Código de Defesa do Consumidor, art. 4º, inciso II, princípio da boa-fé objetiva. Respeitado esse princípio, a

oferta vincula o fornecedor de produto ou de serviço.

Aconteceram dois casos recentes, muito interessantes, talvez os senhores tenham acompanhado pela internet ou pelo noticiário. Um deles aconteceu com a FNAC, uma livraria muito grande, que possui no Brasil seis ou sete lojas físicas, além de um *e-commerce* bastante ativo. Em determinada data, a FNAC, por volta de meia noite, foi atualizar seu site e colocou à venda uma TV de plasma e um computador MacBook da Apple por R$ 9,99 (nove reais e noventa e nove centavos) cada. As pessoas que conseguiram acessar o site, que ficou no ar por mais ou menos trinta minutos, compraram inúmeras televisões e inúmeros computadores. Umas ligavam para as outras e todo mundo comprou. Quando a FNAC percebeu o erro, tirou a página do ar, enviou uma carta aos clientes dizendo que, lamentavelmente, não poderia entregar os produtos porque se tratava de um erro e que gostaria que todos entendessem. Os consumidores não aceitaram, porque a oferta vincula o fornecedor. Tem boa-fé quem compra uma TV de plasma de 52" e um *notebook* da *Apple* por R$ 9,99 (nove reais e noventa e nove centavos) cada um? A boa-fé de que trata o art. 4º do Código de Defesa do Consumidor aplica-se às duas partes da relação, não somente à boa-fé do fornecedor, mas também à do consumidor. A oferta foi feita, mas se tratou de um evidente equívoco. Aliás, um equívoco que o Prof. Rizzato Nunes parece que já imaginava que aconteceria, porque, em seu livro "Manual de Direito do Consumidor", cita exatamente o exemplo da televisão: uma loja que erra e, em vez de cobrar R$ 500,00 (quinhentos reais), cobra R$ 5,00 (cinco reais). **Mutatis mutandis**, foi o que aconteceu com a FNAC. Então, provocaram o Judiciário, que entendeu não haver princípio da vinculação da oferta nessa hipótese por falta da boa-fé. Portanto, quando se fala em oferta, deve-se fazer a leitura de boa-fé.

Por outro lado, em um exemplo que ocorreu em várias cidades do Estado de São Paulo, o Supermercado Makro, um grande atacadista, distribuiu um folder, fez publicidade na TV e fez publicar na Folha de São

Paulo a oferta de um *notebook* por R$ 899,00 (oitocentos e noventa e nove reais). Quando as pessoas chegavam na loja, descobriam que havia um erro. Foi fixado um cartaz gigantesco na loja dizendo que se tratava de um equívoco, que o preço era R$ 1.899,00 (um mil oitocentos e noventa e nove reais). Tem boa-fé quem pretende comprar um notebook por R$ 899,00 (oitocentos e noventa e nove reais)? Atualmente, tem; há dez anos não, porque um notebook não custava esse valor. O Makro foi abrigado a sustentar a venda por R$ 899,00 para todos os consumidores que reclamaram da oferta não atendida.

O terceiro item dos requisitos de formação é a aceitação, ou seja, o dever de cumprir; é um item do contrato eletrônico, como é do contrato físico, normalmente.

Uma questão muito polêmica é o local da formação do contrato. Passarei algumas orientações, inclusive sobre os tipos de contrato, com seu local de formação.

Consta do slide o seguinte: qual lei será aplicada? Qual o local de formação desse contrato, portanto?

Se o contrato for interpessoal, a regra é que a lei aplicada seja o art. 435 do Código Civil, que diz: "Reputar-se-á celebrado o contrato no lugar em que foi proposto." Portanto, se for um contrato interpessoal, o local da proposta. Às vezes, temos dificuldade de identificar onde é efetivamente essa proposta, pois foi encaminhado por *e-mail*, e recebido em outro *e-mail.* O lugar da proposta é a saída caixa de correio ou a recepção na outra caixa? Ou, ainda, o período que o e-mail ficou parado na nuvem? É algo tormentoso. Não sei qual o momento efetivo da proposta.

Para resolver essa questão, temos o art. 9º, § 2º, da Lei de Introdução ao Código Civil, que diz o seguinte: "A obrigação resultante do contrato reputa-se constituída no lugar que residir o proponente." Assim, podemos determinar o lugar do contrato como o lugar que residir o

proponente.

E se o contrato for interativo, pessoa X sistema, tenho uma possibilidade bem grande de pensar em diversos lugares.

Observem este desenho:

Local 1: titular do *site*. Nesse caso, p proponente é sistema X pessoa

Local 2: registro do domínio.

Local 3: servidor.

Local 4: cliente/usuário.

Nos casos de contratos interativos, sistema X pessoas, a maior discussão está, de fato, em qual local aceito. Para resolver esse dilema, recorro à Lei Modelo da UNCITRAL, criada em 1996, nos Estados Unidos, que serve para regulamentar o comércio eletrônico internacional.

O art. 15 dessa lei diz o seguinte:

> Salvo convenção em contrário entre o remetente e o destinatário, uma mensagem eletrônica se considera expedida no local onde o remetente tenha seu estabelecimento e recebida no local onde o remetente tenha seu estabelecimento. Para fins dos seguintes parágrafos:
>
> a) se o remetente ou o destinatário têm mais de um estabelecimento, ou se seu estabelecimento é aquele que guarde a relação mais estreita com a transação subjacente ou, ainda, caso não exista uma transação subjacente, o que vale é o estabelecimento principal.

A primeira informação da UNCITRAL é o estabelecimento principal do remetente ou do destinatário. Se ele tiver mais de um local, por exemplo, local do servidor, local domínio e local físico, vale o estabelecimento principal. A segunda informação, que é a que garante uma discussão mais tranqüila: se o remetente ou destinatário não possuir

estabelecimento, ou se houver dúvida, levar-se-á em conta a sua residência habitual.

A UNCITRAL traz a regra aos contratos interativos e considera o seguinte: estabelecimento do remetente ou destinatário, como primeira regra; se não houver estabelecimento, residência habitual. É o que está sendo usado para dirimir esses conflitos de local da efetivação do contrato.

4.5.1 - FORO PARA DIRIMIR CONFLITOS

-art. 111 CPC – eleição das partes

- art. 94 CPC (ação pessoal) – domicílio réu

- art. 100, IV, d, CPC (exigência da obrigação) – local onde a obrigação deve ser satisfeita

- Contrato de consumo: art. 101 CDC – domicílio do consumidor (defesa do consumidor) ou domicílio do réu (fornecedor autor).

Outro conflito interessante diz respeito à competência do foro. Qual o foro competente para dirimir os conflitos? Se houver eleição das partes, o foro competente é o de eleição, previsto pelo art. 111 do Código de Processo Civil; se não houver eleição de foro – como estou tratando de uma obrigação pessoal –, aplico o art. 94 do Código de Processo Civil, que considera competente o foro do domicílio do réu por se tratar de obrigação de ação pessoal. Se for para exigir o cumprimento de uma obrigação, o art. 100, IV, d, do Código de Defesa do Consumidor, diz que é o local onde a obrigação deve ser satisfeita.

Vale observar que se o contrato for de consumo, o art. 101 do CDC traz uma garantia bastante interessante: para o contrato de consumo, se for um direito postulado pelo consumidor, o foro

5 – CONTRATO ELETRÔNICO DE CONSUMO

5.1 Vulnerabilidade eletrônica

5.2 – Relação jurídica de consumo na internet

5.3 – Contrato de adesão

5.4 – Direito de arrependimento

competente é o domicílio do consumidor. Na hipótese de ser um direito postulado pelo fornecedor, aplica-se a regra do domicílio do réu, também o domicílio do consumidor, só que a fundamentação é diferenciada.

Quanto ao contrato eletrônico de consumo, gostaria de dizer que o princípio da vulnerabilidade, previsto no *art. 4º, inciso I*, princípio que rege o Código de Defesa do Consumidor, diz que todo consumidor é vulnerável - é uma presunção absoluta do legislador na Lei nº 8.078/90 – começa a ganhar um novo contorno.

A Professora Cláudia Lima Marques, uma das maiores consumeristas do País, professora titular na Universidade Federal do Rio Grande do Sul, doutorada na Alemanha, que traz excelentes obras sobre o direito do consumidor, diz que surge uma nova modalidade de vulnerabilidade, a vulnerabilidade eletrônica.

No contrato eletrônico de consumo existe a presunção absoluta de que o consumidor é vulnerável. Essa vulnerabilidade é chamada de vulnerabilidade eletrônica, ou seja, o consumidor é a parte mais fraca na relação de consumo eletrônico. Nessa hipótese, falo de uma relação entre consumidor X negócio, B2C (*business to consumer)* e não entre particulares. Nesse caso, o princípio da vulnerabilidade é plenamente aplicado como a vulnerabilidade eletrônica como reconheceu a Professora Cláudia Lima Marques.

Não há dúvida de que o contrato eletrônico está sujeito ao CDC. Conforme o art. 2º: consumidor é toda pessoa física ou jurídica – não está na lei, mas pública ou privada – que adquire ou utilize produto ou serviço; art. 3, **caput**: fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

Se tenho entre eles um produto, um bem móvel ou imóvel,

corpóreo ou incorpóreo, ou um serviço, qualquer atividade colocada no mercado de consumo, mediante remuneração, mesmo as atividades de natureza bancária, securitária, financeira ou de crédito, há uma relação de consumo, portanto. Preenchidos esses requisitos não há dúvida de que o contrato eletrônico está sob a égide do CDC, portanto aplicam-se todas aquelas garantias das cláusulas abusivas.

As cláusulas abusivas podem ser declaradas nulas, de ofício, pelo juiz, com exceção de uma, cláusula abusiva nos contratos bancários, que o Superior Tribunal de Justiça, em súmula recente, entendeu que tem que ser a requerimento das partes, Súmula nº 378, se não me trai a memória.

Falei um pouco de contrato de adesão e o CDCr trata dessa possibilidade, com a análise de que o contrato deve ser verificado de forma mais benéfica ao consumidor, sempre que houver alguma discussão.

O quarto elemento que trago para falar de contratos eletrônicos é um direito que considero fantástico, o direito de arrependimento. O CDC, art.49 traz a possibilidade do arrependimento, se a compra foi realizada fora do estabelecimento comercial e cita alguns exemplos: catálogo, telefone, residência, lógico que ele não falou de internet, nem precisava; a compra realizada na internet é considerada fora do estabelecimento comercial, embora, tenha consideráveis autores que entendam que não, o que já está pacificando-se.

Para essa compra realizada fora do estabelecimento comercial, o consumidor tem o direito de arrependimento no prazo de sete dias da entrega do bem ou da prestação de serviço ou da assinatura do contrato, sem que esse arrependimento tenha que ser motivado.

O que tomamos conhecimento é que, para algumas compras realizadas na Internet, o direito de arrependimento começa parecer abusivo por parte do consumidor. Vou explicar por quê.

Algumas lojas virtuais como, por exemplo: americanas.com,

submarino.com, enfrentam problemas seriíssimos com o direito do arrependimento do art. 49. Um consumidor compra um CD e ao abri-lo em casa, grava-o, coloca-o na caixinha e realiza o arrependimento. Depois ele compra outro CD; abre, grava e arrepende-se. Compra outro, abre, grava e arrepende-se. Compra um livro, lê o livro em dois dias, arrepende-se porque o livro não é tão bom; então, devolve.

Essa situação está dentro do art.49? A rigor está, porque o direito de arrependimento não é motivado. Agora, não demonstra boa-fé uma atitude dessa natureza. Como é que o fornecedor saberá se o sujeito abriu ou não o CD? Isso é fácil, retirou o lacre. Mas só de retirar o lacre já quebra o direito de arrependimento? Como o fornecedor saberá se o sujeito leu ou não leu o livro? Então, o fornecedor começa a enfrentar problemas seriíssimos, porque inviabiliza a atividade comercial.

Não precisa mais vender CD, vai entregando para a pessoa, a pessoa grava e devolve, não precisa nem baixar a música na Internet, nos *sites* que pirateiam as músicas. É só comprar de forma regular, exercendo o seu direito de consumidor, e depois devolve no prazo de sete dias e ponto final.

A jurisprudência do Tribunal de Justiça de São Paulo entendeu que para produtos como CD e DVD, o direito de arrependimento tem a finalidade de impedir ou de afastar a compra de inopino, aquela compra emocional realizada fora do estabelecimento comercial. Esse tipo de compra não tem essa garantia; as mulheres reclamam muito disso, principalmente em relação à compra de sapatos, porque a mulher, logo que sai da loja com a caixa de sapatos, já se arrepende de ter comprado mais um par.

A questão não é o fato de arrepender-se daquele CD ou do conteúdo daquele livro, não é isso, e sim arrepender-se da compra. Então, se o produto foi aberto não se deve exercer o direito de arrependimento. Essa é uma interpretação pautada no princípio da boa–fé, que a lei não prevê. É um tema interessante para saber até que ponto podemos avaliar

se o produto foi aberto ou não, para que o arrependimento possa existir. A rigor, a lei não prevê esse requisito.

A lei prevê outra polêmica em relação ao direito de arrependimento: se o fornecedor, no prazo de reflexão, que é o prazo de sete dias, resolver pela devolução do produto ou do serviço, tem direito de ter de volta toda a quantia paga, a qualquer título, devidamente corrigida.

A qualquer título é algo que me preocupa, porque, por exemplo, um sujeito compra um CD em uma loja dessa natureza e, ao recebê-lo, olha para o CD e diz que está arrependido, que não quer mais e o devolve. Exerceu o direito de devolução, de arrependimento, só que a loja argumenta que está tudo bem, aceita a devolução do CD e devolve o dinheiro, mas comunica que ele terá que pagar o frete. Ao que o consumidor não concorda, alegando que esse arrependimento está previsto no art. 49 do CDC, a devolução da quantia paga a qualquer título, e exige que a loja devolva o dinheiro do frete. É justo o fornecedor arcar com o frete para o arrependimento do consumidor? Se isso for justo, estamos pagando muito mais do que o preço que deveria custar o CD, o DVD, o livro, porque está embutido nesse valor. É obvio que o fornecedor não vai arcar com essa despesa.

O Tribunal de Justiça de São Paulo, em uma decisão que me parece bastante razoável, diz o seguinte: existem duas coisas diferentes, uma coisa é o produto, outra coisa é o serviço. O consumidor exerceu o direito de arrependimento do produto, mas o serviço de frete foi, efetivamente, prestado. Assim, o Tribunal de Justiça de São Paulo entendeu que o valor do frete é devido.

Trata-se de uma análise jurisprudencial interessante, justa, que não inviabiliza a realização da atividade comercial; senão teremos pessoas profissionais em aplicar o art. 49 do CDC. O sujeito pede, ganha, volta, devolve, o dinheiro vai entrando na conta, o que é uma forma de ganhar porque a devolução do dinheiro teria que ser corrigida monetariamente. Então, o exercício do art. 49, que trata do direito de arrependimento, deve

ser analisado também sob a ótica da boa-fé objetiva.

Para finalizar apresento algumas decisões somente para observarmos rapidamente. A idéia não é ficar analisando a jurisprudência, até porque essa leitura é muito cansativa quando é feita no telão, mas somente para analisarmos juntos algumas decisões interessantes.

EMENTA: AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTO. CONTRATO ELETRÔNICO. INEXISTÊNCIA DE FORMA ESPECIAL. IMPOSSIBILIDADE JURÍDICA DO PEDIDO. Em se tratando de contrato eletrônico interpessoal, no qual as partes interagem na manifestação de suas vontades, para a formação do próprio vínculo, independentemente de forma especial, **não há como exigir-se a apresentação do contrato por parte da demandada**, até porque a própria demandante demonstra que os termos do contrato foram livremente deliberados mediante proposta e aceitação por meio de correio eletrônico. Apelo desprovido.

(Apelação Cível Nº 70013028261, Décima Segunda Câmara Cível, **Tribunal de Justiça do RS**, Relator: Dálvio Leite Dias Teixeira, Julgado em 30/03/2006)

Ação cautelar de exibição de documento. Contrato eletrônico. Inexistência de forma especial. Impossibilidade jurídica do pedido. Em se tratando de contrato eletrônico interpessoal – contrato de pessoa X pessoa – no qual as partes interagem na manifestação das suas vontades, para formação do próprio vínculo, independente de uma forma especial, não há como exigir a apresentação do contrato por parte da demandada, até porque a própria demandante demonstra que os termos do contrato foram livremente deliberados mediante proposta e aceitação, por meio de correio eletrônico.

É necessário um contrato em espécie para firmar esse contrato eletrônico? Parece-me que sim. A manifestação de vontade, por *e-mail*, já é indicativo do contrato. Não me parece necessário um contrato específico para demonstrar a vinculação entre as partes.

Estou argumentando que o *e-mail* é uma modalidade de prova. Lógico, a discussão é muito maior, caberia uma palestra específica sobre esse assunto, mas, o *e-mail* é uma modalidade de prova, em um primeiro momento, se não for impugnado.

O Código de Processo Civil diz que o documento pode ser juntado aos autos e será considerado válido se não for impugnado. Então, cabe à

parte contrária impugnar o *e-mail*. A impugnação da parte contrária deve ser em relação, simplesmente, ao conteúdo, porque a forma é válida. Nesse caso, ficou decidido que a forma do *e-mail* era válida para o contrato. Em um primeiro momento fazemos a leitura de que é possível se fazer prova por intermédio de um *e-mail*. Se impugnado, discutir-se-á o conteúdo, sendo necessária uma perícia para ver se houve ou não alteração de conteúdo, partindo para um segundo momento da prova. Portanto, é possível um *e-mail* ser considerado uma prova, assim decidiu o Desembargador Dálvio Leite Teixeira, do Tribunal de Justiça do Rio Grande do Sul.

EMENTA: AGRAVO DE INSTRUMENTO. AÇÃO DE EXECUÇÃO. TÍTULO EXECUTIVO. CONTRATO ELETRÔNICO. CÓPIA. ART. 385 CPC Possível a instrução do pleito executório com a cópia do título, por possuir o mesmo valor probante que o original **quando não impugnada sua fidelidade pela parte contrária**. In casu, o contrato juntado foi formalizado eletronicamente, estando devidamente registrado. Descabe a presunção de irregularidades no documento no presente momento processual. Agravo de instrumento a que se dá provimento, nos termos do § 1º-A do art. 557 do Código de Processo Civil.

(Agravo de Instrumento Nº 70031041155, Vigésima Câmara Cível, **Tribunal de Justiça do RS**, Relator: Angela Maria Silveira, Julgado em 08/07/2009)

Agravo de Instrumento. Ação de Execução. Título Executivo. Contrato Eletrônico. Cópia. Art. 385 do CPC. Possível a instrução do pleito executório com a cópia do titulo, por possuir o mesmo valor probante que o original quando não impugnado sua fidelidade.

Exatamente o que estávamos falando, é válido como prova, salvo se impugnado. Descabe a presunção de irregularidades no documento no presente momento processual.

Nesse caso, o Tribunal de Justiça do Rio Grande do Sul entendeu que a cópia do contrato eletrônico era válida.

CONSUMIDOR – VINCULAÇÃO – OFERTA – BOA-FÉ

EMENTA: CONTRATO ELETRÔNICO. COMPRA E VENDA. PREÇO. DANO MORAL. NÃO CARACTERIZAÇÃO. 1.- Evidenciado que o preço fixado no site se encontra equivocado em face dos demais produtos, mostra-se possível o não acolhimento do negócio realizado. 2.- **A boa-fé deve ser exercida por ambas as partes do contrato**, impossibilidade do contrato gerar locupletamento de uma das partes. Recurso provido para julgar improcedente a ação.

(Recurso Cível Nº 71001490614, Terceira Turma Recursal Cível, Turmas Recursais, **Tribunal de Justiça do RS,** Relator: Eduardo Kraemer, Julgado em 27/05/2008)

Este caso diz respeito

a uma jurisprudência de relação de consumo. Consumidor. Vinculação. Oferta. Boa fé. Observem:

Contrato eletrônico. Compra e venda. Preço. Dano moral. Não caracterização. Evidenciado que o preço fixado no site se encontra equivocado, em face dos demais produtos, mostra-se possível o não acolhimento do negócio realizado.

Trata-se de uma jurisprudência anterior a questão da FNAC, de 2008, portanto, mas que está tratando do mesmo assunto.

A boa fé deve ser exercida por ambas as partes do contrato. Impossibilidade do contrato gerar comprometimento a uma das partes.

Nesse caso, negou-se o dano moral por conta daquela questão da oferta. A oferta é vinculativa, resguardado o princípio da boa fé objetiva do art. 4º do CPC.

Este caso diz respeito a e-*commerce*. Aquisição de impressora por meio de *e-mail* contendo propaganda do produto. Mensagem eletrônica que garantia a entrega do bônus em dinheiro na compra da mercadoria anunciada.

CONSUMIDOR - **E-commerce** - Aquisição de impressora por meio de e-mail contendo propaganda do produto - **Mensagem eletrônica que garantia a entrega de bônus em dinheiro na compra da mercadoria anunciada** - Periférico adquirido que apresentou defeito de fabricação - Fornecedor que se recusou a pagar o bônus anunciado em razão de o produto ter sido trocado por outro similar, alegando, ainda, que a quantia ofertada era de responsabilidade do fabricante - Inadmissibilidade - Publicidade que integra o próprio contrato entabulado entre consumidor e fornecedor - Obrigatoriedade da empresa de comércio eletrônico de efetuar o depósito da verba prometida - Inteligência do art. 30 da Lei 8.078/90.

(ApCiv 70020018529 - **5.ª Câm. Cív. - TJRS** - j. 01.08.2007 - v.u. - rel. Des. Umberto Guaspari Sudbrack - Área do Direito: Civil-Processo Civil/Consumidor.)

Uma pessoa recebeu um *e-mail* que dizia que, ao comparecer com aquele *e-mail* na loja, ela teria um bônus no valor de R$ 200,00 (duzentos reais).

PRESTAÇÃO DE SERVIÇOS - Consumidor - Comércio on-line - Indenização - Dano material - Site destinado à intermediação de compra e venda - Produto adquirido por **meio eletrônico**, com o devido depósito bancário realizado pelo adquirente, e não entregue - **Falha na prestação do serviço evidenciada - Responsabilidade objetiva da empresa de Internet pelo ato lesivo** - Verba devida.

(TJDF - *ApCiv 2006.01.1.113312-4* - 2.ª T. Recursal dos Juizados Especiais Cíveis e Criminais - j. 17.06.2008 - v.u. - rel. Juiz Robson Barbosa de Azevedo - *DJU* 03.12.2008 - Área do Direito: Consumidor.)

Periférico adquirido que apresentou defeito na fabricação. Fornecedor que se recusou a pagar o bônus anunciado em razão de o produto ter sido trocado por outro similar, alegando, ainda, que a quantia ofertada era de responsabilidade do fabricante. – Responsabilidade solidária. CDC – Inadmissibilidade. Publicidade que integra o próprio contrato entabulado entre as partes. Consumidor e Fornecedor. Obrigatoriedade da empresa de comércio eletrônico de efetuar o depósito da verba prometida. Quer dizer, quem fez a venda, relação de consumo, responderá por ela, pois não é responsabilidade do fabricante. Essa foi uma decisão da 5ª Câmara Cível do Tribunal de Justiça do Rio Grande do Sul.

Decisão do Tribunal de Justiça do Distrito Federal:

Prestação de serviços. Consumidor. Comércio *on-line*, Indenização. Dano material. *Site* destinado à intermediação de compra e venda.

Intermediação de compra e venda é praticamente aquilo que chamamos de leilão.

Produto adquirido por meio eletrônico, com devido depósito bancário realizado pelo adquirente e não entregue. Falha na prestação do serviço evidenciada. Responsabilidade objetiva da empresa de internet pelo ato lesivo. Verba devida.

O consumidor pode se valer de uma medida judicial contra o *site* de leilão que impediu a realização do negócio, por falta de segurança, que é uma das exigências na prestação do serviço eletrônico. Portanto, o TJDF sai na frente nessa decisão, que é uma decisão de dezembro de 2008, para reconhecer que o site de leilão tem responsabilidade e não é um mero classificado *on line*, pois ele faz uma intermediação, que é considerada um serviço remunerado e deve que ser prestado com qualidade.

A rigor, o que quis trazer nesse encontro são alguns pontos sobre contratos eletrônicos. Poderíamos aprofundar no que tange aos

documentos e falar um pouco da certificação digital, ou no que tange à doutrina, principalmente em relação à questão da Lei da UNCITRAL, lei modelo nos Estados Unidos, no que tange à doutrina francesa, mas pretendi que este primeiro encontro fosse um pouco mais tranqüilo e mais razoável para dar um norte aos senhores. Gostaria de vê-los, pelo menos parte dos senhores, estudando mais o tema conosco.

Sou Diretor Pedagógico da Rede de Ensino Luiz Flávio Gomes (LFG) e Coordenador da Pós-graduação de Direito Eletrônico, que começará em setembro, em que vamos estudar as relações do Direito Eletrônico com todas as outras áreas do Direito. Vamos ter módulo de Direito Constitucional/Eletrônico; Módulo de Direito Civil/Eletrônico; Trabalho/Eletrônico; Tributário/Eletrônico; Criminal, penal/Eletrônico; Prova forense/Eletrônico.

Mais do que isso. Vamos ter um módulo de aulas técnicas. Quando se fala, por exemplo, em certificação digital, preciso entender o que é certificação do ponto de vista jurídico e técnico. É preciso entender o que aquele sujeito de TI fala sobre a certificação digital. Quando falo, por exemplo, de *e-mail* como meio de prova, preciso entender de que forma consigo identificar a origem de um *e-mail*, o que é uma aula técnica. Vamos ter módulos técnicos entre os módulos jurídicos.

A idéia é desenvolvermos um pouco mais esse processo do Direito Eletrônico, que está cada vez crescendo mais, com profissionais brilhantes, como os Professores Rony Vainzof e José Carlos Almeida Filho que estiveram aqui ontem, e o Professor Augusto Rossini que estará aqui hoje e que são excelentes profissionais nessa área, como a Dra. Patrícia Peck, enfim, só para citar alguns sem ter o objetivo de deixar alguém de fora.

Se os estimulei para estudarem esse tema, o meu papel foi cumprido.

Muito obrigado pela atenção. Bom dia.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Boa tarde a todos. Retornamos com as palestras do Seminário de Direito Eletrônico.

O Seminário de Direito Eletrônico é uma iniciativa do Superior Tribunal de Justiça e do Instituto dos Magistrados do Distrito Federal (Imag-DF).

Nesta segunda parte, teremos a palestra *Crimes Eletrônicos*. Para ministrá-la, convidamos o Dr. Augusto Rossini.

O Dr. Augusto Eduardo de Souza Rossini é Doutor e Mestre em Direito Penal pela Pontifícia Universidade Católica – PUC/SP, Bacharel em Direito pela Universidade Mackenzie; Promotor de Justiça desde 1989, atuando exclusivamente na área criminal desde 1992; atual Coordenador do Centro de Apoio Operacional à Execução e das Promotorias de Justiça Criminais do Estado de São Paulo (CAOCrim); Presidente da Associação Nacional do Ministério Público Criminal; nomeado, em 2002, pelo Ministro da Justiça para compor a Comissão de Juristas para Reavaliação da Lei nº 9.099, de 1995; palestrante, professor permanente no Curso de Mestrado em Direito da Sociedade da Informação e na Graduação das Faculdades Metropolitanas Unidas; atividade docente em diversas instituições nas disciplinas de Direito Penal, Direito Processual Penal e Direito Constitucional; e como convidado da Escola Superior da Magistratura, da Escola Superior da Advocacia, da Escola Superior de Polícia e da Associação dos Advogados do Brasil; autor do livro *Informática, Telemática e Direito Penal*, e co-autor do *Manual de Direito Eletrônico em Internet*; vencedor do *Prêmio Innovare*, com a prática denominada *Promotoria Comunitária*.

Com a palavra o Dr. Augusto Rossini.

PALESTRA VII: CRIMES ELETRÔNICOS

AUGUSTO EDUARDO DE SOUZA ROSSINI
Doutor e Mestre em Direito Penal – PUC/SP
Promotor de Justiça do Estado de São Paulo

Boa tarde a todos e a todas. Primeiramente, agradecemos a oportunidade a esta Casa que nos recebe. Comentávamos: "Aquele office-boy de cartório, fazendo uma palestra no STJ, é o 'sonho de consumo' de todos". Desculpem, mas aquele menino, apesar de toda a nossa trajetória, ainda não nos deixou. Desde aquela época, já tínhamos uma preocupação grande com relação ao tempo dos outros. Se não gostamos que tomem o nosso tempo com assuntos desimportantes, esperamos não fazê-lo com relação ao tempo dos senhores. Atuamos como promotor há 21 anos, dos quais dezesseis em júri. Esse é o nosso pecado; não, a nossa vaidade. A nossa vaidade é tentar construir projetos. A última vaidade foi o *Prêmio Innovare*, com a prática *Promotoria Comunitária* – cujo tema não tem a ver com a questão acadêmica de que trata esta palestra. Esperamos não tomar o tempo dos senhores, que tenha utilidade o que vamos dizer.

Obrigado ao STJ e à Imag-DF. Também agradecemos, na pessoa da Carolina, a todos que de alguma forma construíram este Evento.

Estamos tentando construir uma Teoria do Crime Digital. Aliás, não de "Crime Digital", mas de "Infração Penal Digital", de "Delito Digital". Se usarmos a expressão "Crime Digital", estarão fora as contravenções, a "bola de neve", os jogos de azar e os cassinos. Temos que ampliar o espectro de denominação, para nos referirmos a infrações penais ou a delitos, numa doutrina mais antiga.

Em 1997, era coordenador, a função que exerço hoje, um cargo político: quando muda o procurador, quem o ocupa esse cargo também sai ou acompanha-o, se for convidado. Em Atibaia, uma cidade satélite da Grande São Paulo, surgiu uma investigação policial com relação a um biólogo, formado na Universidade de São Paulo (USP), que mantinha uma página bem estranha na internet. Foram feitos alguns pedidos de providências para a polícia local, em virtude do fato desse rapaz, além de estar na internet, embora sendo biólogo, trabalhar como monitor de recreação, nos finais de semana, em alguns sítios que acolhiam crianças. Era estranho alguém com aquele currículo querer trabalhar em tais ambientes.

A partir da troca de informações, houve uma investigação.

Quando participávamos do Centro de Apoio do Ministério Público do Estado de São Paulo, – que é mais ou menos um arsenal, ao qual quem está tomando tiro na trincheira pede informações –, recebemos um pedido de informação a respeito desse caso, relatando que a polícia havia ido à casa do biólogo e apreendido o seu computador. Ocorre que, como o suspeito já usava criptografia de terceira ou quarta geração à época, o Instituto de Criminalística do Estado de São Paulo não conseguiu acessar os documentos, quer dizer, não abriu os "arquivos *log*", porque não se tinha ainda uma cultura de manutenção da prova.

Não fosse um investigador ter aberto as gavetas – tal permissão constava da ordem judicial – e apreendido algumas fotos e documentos, esse sujeito não teria sido condenado a onze anos de prisão por atentado violento ao pudor.

Esse caso nos chamou muito a atenção: "Do que se trata? Está surgindo um fenômeno?"

O primeiro caso de crime digital no Brasil foi a ameaça às jornalistas Bárbara Gancia e a Maria Cristina Poli, em 1992/1993, em que

o Delegado Mauro Marcelo Lins e Silva, ex-Diretor da Agência Brasileira de Inteligência (Abin), identificou o autor do crime, e conseguimos puni-lo.

Com tudo isso, pensei ter encontrado o tema para a minha tese de doutorado. Fui então falar com o meu orientador, Dr. Dirceu de Melo, à época Presidente do Tribunal de Justiça, que me disse para discorrer sobre culpabilidade, porque aquele assunto não era adequado.

Notem no que se transformou esse tema: uma tese de doutorado; que, aliás, encontra-se à disposição dos interessados.

Estávamos procurando um tema para a nossa tese de doutorado e encontramos. De lá para cá, não paramos mais de falar desse assunto, viramos professor e até escrevemos alguns livros a respeito. Isso porque "em terra de cego, quem tem um olho é rei". Ou seja, saímos na frente na pesquisa desse assunto. Inclusive, dissemos, agora, em entrevista que esse estudo não iria parar, porque o que era um feixe grande virou algo segmentado, onde falamos em prova, em processo eletrônico, em tipo penal. Aliás, nesse sentido é que começamos a dividir o assunto, para começarmos a falar propriamente da apresentação.

Há um texto, publicado pela Editora Atlas, há poucos meses, em que sugerimos para o tema a denominação: "Tutela Penal da Sociedade da Informação". A utilização da expressão "Tutela Penal" justifica-se porque abarca tanto a tutela do direito material quanto a tutela do direito adjetivo. Essa denominação abrange tanto o que está fora quanto o que está dentro da rede, porque há crimes como, por exemplo, o "chupa-cabra" em ATM, que é um crime informático, mas não é um crime telemático se não houver o uso do cartão na rede.

Separamos o tema em três grandes feixes, em três grandes pilares: tipo, o direito material; prova, a coleta da prova; e o processo eletrônico; embora a prova pudesse estar na espécie do gênero processo, mas para essa classificação os assuntos não se misturam. Tipo penal, que refere-se ao direito material; processo, processo eletrônico, e a prova

digital, tema da próxima palestra, a ser ministrada pelo Dr. Ulysses Alves de Levy Machado.

O tema da presente palestra será uma proposta de teoria dos crimes, das infrações penais digitais.

A intervenção do Estado, leia-se: quem tem a titularidade do **jus puniendi**, chegou tarde neste ramo do conhecimento. Esse é um grande problema, que não sabemos se iremos resolver.

Não posso desceremos a minúcias dessas revoluções, mas o que nos interessa, nesse olhar, são as revoluções tecnológicas, as revoluções intelectuais, que afetarão fortemente o Direito, em geral, e, em especial e fundamentalmente, o Direito Penal.

Nas duas últimas eras a que nos referimos, a da Informática e a Digital – aliás, a elétrica ou eletrônica, um pouco antes –, ainda acontecem no Brasil. O Governo federal tem um programa chamado Luz para Todos, que nada mais é do que o acesso à energia elétrica. É uma revolução para a mulher que passa roupas com o ferro de brasa passar a fazê-lo com o ferro elétrico. O que pode parecer desimportante para quem não passa roupas. Imaginem, por exemplo, como é difícil fazer comida sem geladeira. É *punk* não ter energia elétrica em casa.

Agora, *punk* é não ter energia nem computador. Nós, o Dr. Ulysses e alguns jovens "há mais tempo" aqui presentes, vamo-nos lembrar do quanto era difícil ter dinheiro no fim de semana se não passássemos antes no caixa do Banco do Brasil ou da Caixa Econômica Federal, por exemplo. Era difícil. Caso não tivéssemos amizade com o dono da padaria ou com o

dono do posto de gasolina, não teríamos como gastar. Hoje, não há essa necessidade, pois tudo já está incorporado.

A era digital, em síntese, é a conversa de uma máquina com a outra.

Não nos damos conta das revoluções porque as vivenciamos. Todos aqui já vivenciaram-nas. Agora, o que nos interessa é o que chamo no trabalho de "a cobra comendo o rabo". Que maluquice é essa? Os americanos, na década de sessenta, tinham uma preocupação muito grande com relação à possibilidade de serem atacados pelos russos a partir de Cuba, durante a chamada Guerra Fria. Com muito esforço, criaram uma teoria, uma forma de proteger as informações que estavam no Pentágono e nos quartéis, valendo-se da Teoria dos Fractais e da Teoria do Caos, um sistema em que as informações estivessem em todos os lugares a todo tempo, nos *hosts*, criando os nós. As informações ficavam segmentadas, empacotadas, em alguns lugares para unirem-se em outros lugares e poder fornecer a informação total, quando do interesse do Governo norte-americano.

Soberania e interesse militar nasceram no seio militar. E essa forma de tratar a informação – que era boa porque possibilitava a troca de informações entre quartéis e entre centros de inteligência, preservando a informação – foi para a universidade. Foi nesse momento que Steve Jobs e Bill Gates, dono da Microsoft, faturaram bastante, ao perceberem a oportunidade de trazer essa ferramenta para a universidade, possibilitando às universidades norte-americanas e européias conversarem entre si.

Depois, essa ferramenta veio para o mercado. E aí é onde digo que "a cobra mordeu o rabo". Vivemos o neoliberalismo; uns, muito novos, outros, não; mas vivemos. Lembremo-nos quando o presidente Collor falava que nossos carros eram carroças, que devíamos abrir o nosso mercado para o mundo. Era a abertura do mercado, o neoliberalismo, o novo liberalismo. E liberalismo é o não-Estado. A internet optou pelo não-

Estado, pelo caminho da autorregulamentação. Tanto é que os registros de domínios, até dois ou três anos atrás, era feito pela Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), um organismo de educação, da secretaria de educação de uma faculdade. O registro do domínio ocorria numa faculdade pela lógica da Segunda Onda – não da Terceira.

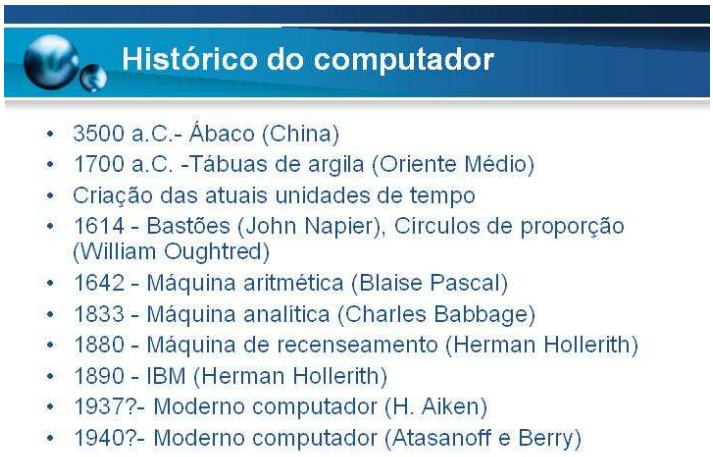
Quando chega ao mercado, acontece do jeito que os americanos queriam: vamos lá, vamos vender, vender, vender. E, então, os "caras que deixam a barba grande", os terroristas da Al Qaeda, querendo ferir de morte a cultura econômica mercantilista, atacaram as Torres Gêmeas e o Pentágono. Notem o paradoxo.

A forma com que os terrorista se comunicavam, sem que ninguém percebesse, é de uma singeleza que dá raiva: abriam uma conta única, com cinco ou dez participantes, todos com acesso à senha, e conversavam pelo rascunho. Básico, não? Não trocavam *e-mails* entre si. Ou seja, foram ao seio norte-americano e bombardearam dois prédios usando a mesma ferramenta criada pelos próprios americanos para invadir o mundo com a economia. Portanto, "a cobra comeu o próprio rabo".

O atentado às Torres Gêmeas ocorreu em 11 de setembro de 2001; em 23 de novembro de 2001, a Comunidade Européia, na Convenção de Budapeste, construiu uma normativa internacional para a Europa, tipificando doze condutas e vários procedimentos de prova. O Brasil não é signatário dessa Convenção, porque não tem todos os tipos ali previstos; não consegue se adequar, porque o projeto de lei do Senador Eduardo Azeredo não tramita no Congresso.

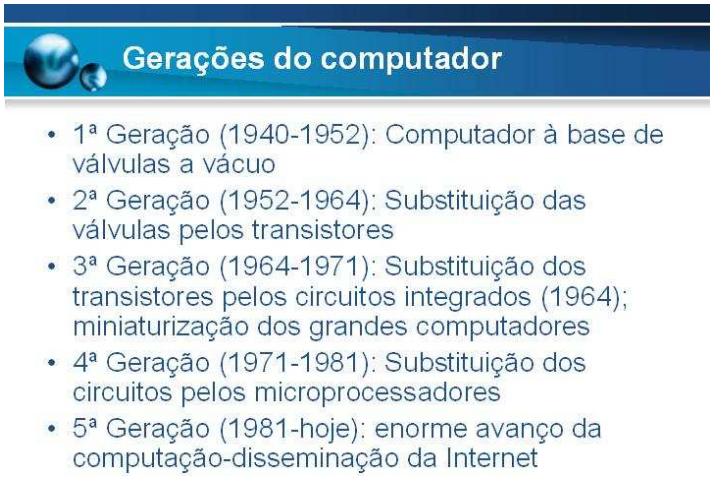
Os americanos foram assinar uma convenção em Budapeste, e não em Nova York ou em Washington, porque era a que tinha para mudar a cultura. Aí quiseram correr atrás e a coisa pegou. O *gap*, a distância entre o estado e o mercado e a internet, nunca mais será alcançado. Por isso sustentamos a prevenção e não a repressão. O estado não chegou a tempo adequado de construir um sistema de proteção e de repressão, na

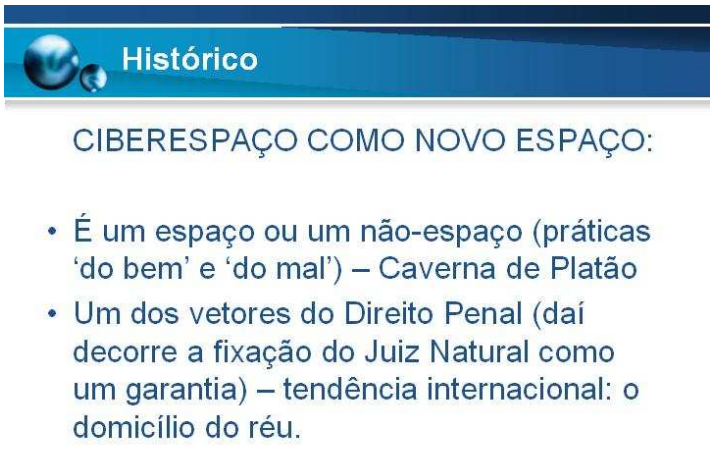
medida em que os fatos ocorrem. Chegamos, mas não em tudo. Aliás, é impossível, porque não há controle, é do negócio da internet não ter controle. Se fosse ser rigoroso com o Código Penal, o art. 307, que se refere à falsa identidade, seria o artigo que mais se denunciaria na rede. Quem não usa *nick* na internet? Quem não teve uma página na internet meio suspeita? Não podemos falar, mas é o que acontece. E a dúvida é: será esse o Direito Penal que queremos? Esta é a busca: o que podemos e o que não podemos aplicar e o que temos que construir para resolver alguns problemas.



Esse é o histórico do computador. Demonstramos, nesse *slide*, o esforço da humanidade no sentido de economizar tempo. E o paradoxo aparece novamente: economizamos tempo e realizamos mais tarefas. Quem poderia imaginar que um dia iríamos trabalhar a distância? Antes, ao chegarmos de uma viagem de um avião, esperávamos o avião pousar, íamos ao saguão do aeroporto, ou ao chegar ao hotel, e ligávamos. Atualmente, de dentro do avião, já mandamos um torpedo para avisar que chegamos.

Só que tudo de bom que estamos vivendo também é usado pelo outro lado. Essas facilidades expressas pelas gerações do computador, sendo que a 5ª Geração vem de 1981 até os dias de hoje. Há ainda uma 6ª Geração a ser acrescida, denominada Geração da Nuvem.





Neste ponto começamos a ter alguns problemas. Temos uma história e um novo espaço. Os sociólogos usam a expressão "não-espaço", que está ligada à modernidade de uma forma muito clara, são os aeroportos, as estações, aqueles espaços que o Direito sempre tratou ficcionalmente: se acontecer um homicídio em um avião que esteja sobrevoando o Oceano Atlântico, a competência para julgar este crime será da justiça do local onde o avião pousar. Isso é ficção. O homicídio ocorreu sobre o oceano, não há jurisdição. Construímos todo o resto para dar juiz natural àquela causa.

Aliás, encontramos vários exemplos de ficção no Código Penal e no Direito em geral. Sustento que o não-espaço é ficcional. Platão, no *Mito da Caverna*, descreve uma comunidade que nascera dentro de uma caverna e só vira o mundo por sombras; é mais ou menos o que ocorre com a internet: lá somos bonitos, ricos; temos outros espaços, até tribunal; no *Second Life*, somos tudo o que quisermos; na vida real, não assumimos,

"estamos no armário", não saímos; mas, na internet, estamos fora, indo a festas *rave*, e de *gay*. Nada contra, mas somos o que queremos ser, porque projetamos lá.

Mas será que aquilo que acontece na internet tem reflexo aqui? É isso que estamos descobrindo.

Três exemplos de ficção. Crime continuado. Existe crime continuado? Política criminal. Inexiste, é uma opção do legislador. Se vários crimes forem praticados em circunstâncias de tempo, num território, com o mesmo **modus operandi***,* todos os outros entendem como continuação do primeiro. Mentira, não existem, é pura ficção, uma opção criada pelos monges copistas, na Idade Média.

À época em que, após o terceiro crime, o autor era levado à morte, os canonistas diziam que se precisava de gente para o mundo, e, portanto, as pessoas não podiam ser mortas. Surgiu, então, a ideia de interpretar os crimes: se fossem parecidos, resumir-se-iam a apenas um. Daí, nasceu o instituto do crime continuado. Crime continuado é ficção, não existe. É opção do legislador.

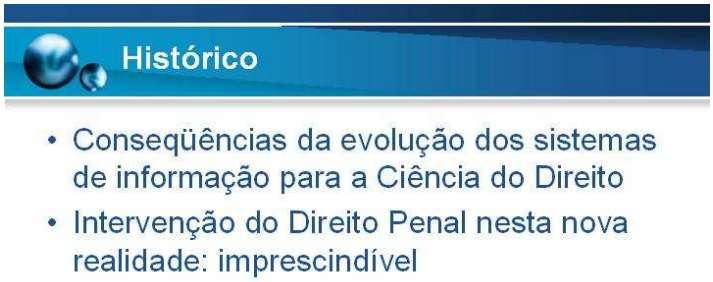
Só tem dois tipos de concurso de crimes, no mundo fenomênico, no mundo das pessoas: concurso material e concurso formal. Tendo várias condutas e vários resultados, concurso material; com uma conduta e vários resultados, concurso formal. É assim. Dirigindo um ônibus com cinquenta servidores do STJ, morre todo mundo, houve uma conduta com cinquenta resultados; entro aqui, saiu dando tiro em cinquenta servidores, um de cada vez, concurso material. O resto é ficção.

Outra ficção constante do Código Penal: **actio libero in causa**, art. 28, § 2º. Alguém se embriaga e dorme por cima do filho, que morre asfixiado. Havia culpabilidade durante o sono? Nenhuma. Temos as três fases da bebida, conforme estudamos em Direito: a fase do macaco, a fase do touro e a fase do porco. Na fase do macaco, quem bebeu fica dando risada – nessa fase, já se caracteriza o crime do art. 306 do Código

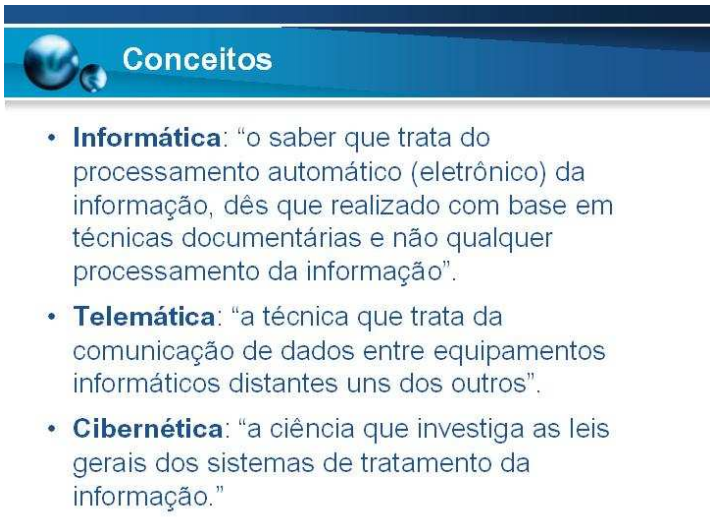
de Trânsito Nacional. Na fase do touro, o bêbado quer brigar. Na fase do porco, o embriagado vira e fica – mas pode cometer crimes durante esse período. Há culpabilidade? O legislador diz que, se beber, pagará pelo que fez durante o seu período de embriaguez. Isso é ficção, não tem culpabilidade. Mas, para não transformar o ato numa conduta impune, o legislador estende a culpabilidade.

A teoria do erro também é ficcional. Erro: alguém intenciona matar o mestre de cerimônia do Evento, porque o apresentou de forma errada; contudo, mata outrem. Todo dolo, toda a torpeza se transfere para a outra pessoa. **Aberratio ictus**. Alguém pretende matar uma pessoa e atinge outra. Querendo matar alguém, por motivo fútil, atinge outro. Todo dolo, toda vontade que o agente dedicava em relação ao primeiro, toda a motivação, transfere-se para a pessoa que foi atingida. No mundo fenomênico, trata-se de uma tentativa de homicídio por motivo torpe, com relação ao primeiro, e dolo eventual, com relação ao segundo, porque se assumiu o risco de produzir resultado, como ao atirar-se com alguém atrás. Mas não, o legislador disse que se transferem todas as circunstâncias elementares e subjetivas para o resultado: responsabilidade objetiva, ficção.

Internet: ciberespaço também é ficção. Onde está o ciberespaço? Mas há crimes próprios da internet. Teremos que construir. Aliás, o Código Penal, além da Teoria Geral, na parte especial, também coloca várias ficções; os crimes de perigo estão sendo criticados, porque para se ter a conduta não é necessária a existência do resultado danoso.



Temos que pensar e refletir se há condições ou a necessidade de trazer esse tema para a Ciência do Direito – se é que Direito é ciência. Há quem diga que Direito nem ciência é, como o Professor Doutor Tércio Sampaio Ferraz Júnior, catedrático de Filosofia pela USP, que diz que Direito é técnica e não ciência. Mas o fato é que o Direito Penal é o direito da sanção, o direito da pena, o direito da algema, o direito da repressão, de cercear a liberdade. Perguntamos como, neste mundo do *laissez-faire*, do deixar fazer, do descontrole, vamos aplicar o controle do Direito Penal. É um grande problema. Temos que ter todas as cautelas que o sistema nos fornece: anterioridade, tipicidade e o devido processo legal, quando formos fazer a prova. Então, passamos a pensar que o Direito Penal tem que interferir, porque os fatos já o dizem por si e as pessoas já estão sendo presas. Há pessoas que praticam condutas danosas em relação às outras, embora em ambiente virtual.



São tantos os conceitos que até pedi para uma aluna de mestrado elaborar um trabalho abordando o tema. Encontramos conceitos em vários contextos. Por exemplo, são abundantes em conceitos: o art. 16 do Projeto de Lei do Deputado Luís Piauhylino; o Projeto de Lei do Código Penal, de 1997, da reforma da parte especial, de autoria do Jurista Miguel Reale Júnior, e que contém o conceito de documento eletrônico; a Convenção de Budapeste; e aqui apresentamos os conceitos necessários para tratarmos o tema.

Informática é um saber do controle dos dados, do processamento eletrônico da informação. Tratando deste conceito, temos a Ciência da Computação. É enorme este campo do conhecimento.

Existem crimes ou condutas apenas informáticos. Já tínhamos conhecimento disso quando os computadores começaram a chegar. Por exemplo, o caso das escrituras falsificadas, feitas em computador – não é caso de telemática.

Até hoje chegam à Promotoria Criminal fraudes relativas à autenticação por caixa eletrônico. Alguém paga uma conta, tem o recibo, a prova, mas não houve o pagamento. Esse é um exemplo de crime informático, pois não entrou na rede. Telemática é uma técnica que gera troca de informações entre computadores, e, nessa hipótese, rompemos, com a telemática, diretrizes, bases fundamentais do Direito Penal.

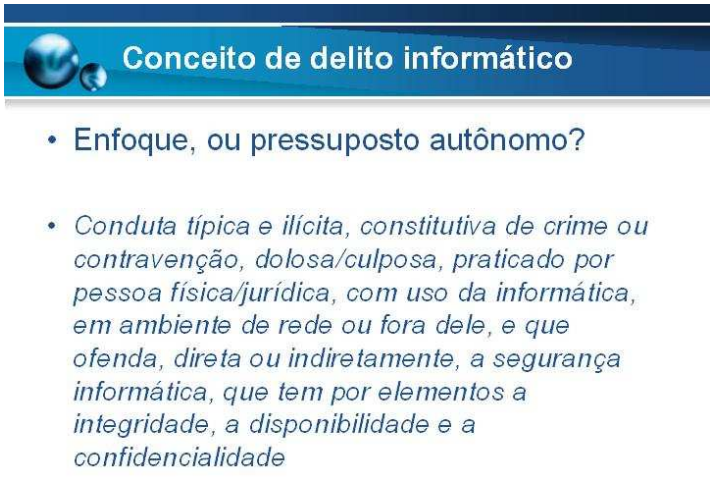
Local. O local do crime. Se abrirmos o Código encontraremos os princípios da legalidade e da anterioridade; em seguida, o tempo em que ocorreu e o local do crime. O Código tratar do tempo e do local do crime já nos seus primeiros artigos, porque, numa interpretação sistêmica,

esses conceitos têm importância fundamental para saber-se de prescrição, de qual a lei que se aplica naquele tempo e do local do crime.

Cibernética relaciona-se com o conceito de governança, é *kubernétikê* em grego; é a ciência que investiga as leis gerais do sistema de tratamento da informação.

Então, tanto a telemática quanto a cibernética rompem – o crime cibernético, o crime digital ou qualquer denominação que se queira –com os vetores espaço e tempo.

Elaboramos um conceito de crime informático, que está à disposição dos senhores.



Encontramos vários tipos de classificação de delitos de informática, como as categorizações de Ulrich Sieber, de Klaus Tiedemann, em 1984, que cita crimes econômicos e bancários; e a classificação do Professor Scarance – que nos cita, quando ainda utilizávamos uma classificação tripartite.

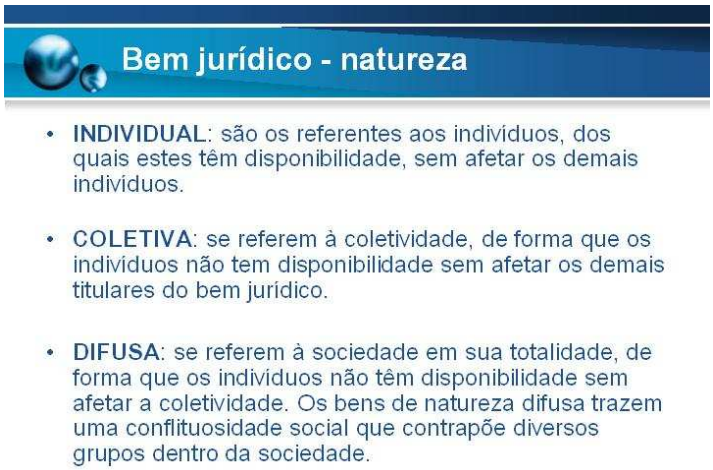
Atualmente, entendemos que a classificação deve incluir apenas os delitos puros e os delitos mistos, pela singeleza. Simples: delitos mistos

são aqueles que são praticados em quaisquer lugares. Em qualquer lugar temos o estelionato e o crime contra a honra. O que não ocorre com o crime de invasão de sistema, que é uma conduta atípica, como gênero. O art. 72, da Lei nº 9.504, o Código Eleitoral, menciona a invasão de sistema na apuração eleitoral, com pena de reclusão de cinco a dez anos. Este é um crime informático puro, porque só pode ser praticado em ambiente de rede.

Então, o delito puro tem por natureza que ser praticado na rede de computadores. Só temos como tipificar esse tipo de crime – como explicamos há pouco – pela via da ficção. Não há como visualizar a conduta, mas apenas o que for exteriorizado. Por exemplo, a invasão de sistema, no Brasil, não consta da parte especial do Código. Na Itália, a questão foi resolvida acrescentando-se um parágrafo à parte do código que trata do crime de invasão de domicílio: ao conceito de casa abarcou-se o conceito de sistema de computador e deixou-se a interpretação para o hermeneuta – o legislador tem que permitir que trabalhemos.

Ora, se combinarmos o art. 29, referente sobretudo às participações e às coautorias, teremos todo tipo de crime praticado com o uso da máquina, especialmente os delitos mistos, como o crime contra a honra, o homicídio, o estelionato e a ameaça. Se dissermos, por exemplo, que o Professor Ulysses sairá daqui às sete horas da noite, que estará no carro tal, que deverá ser inteceptado em tal lugar e morto com tantos tiros, seremos partícipes de um homicídio; e a prova far-se-á digitalmente, embora seja crime material, com resultado naturalístico.

Não é muito difícil de entender. A dificuldade maior reside na classificação dos delitos puros, pois, primeiro, não estamos acostumados nem com o tipo e nem com a prova; segundo, é difícil de visualizar e de compreender esse tipo de crime como fenomênico.



Se temos a história, o conceito e a classificação, podemos começar a tentar construir uma teoria de crimes dessa natureza, ou de um conhecimento dessa natureza. Para tanto, devemos definir a natureza de bem jurídico, porque, em Direito Penal sem a identificação de um bem passível de tutela do Estado, porque se não for passível de tutela, o problema é de outro ramo, é do Direito Civil, do Direito Administrativo, do Direito Constitucional, e não do Direito Penal. E não só passível de tutela do direito, porque tem muita coisa que é passível de tutela do direito e não é passível de tutela do Direito penal. Ou seja, tem que ser a tal da **ultima ratio** mesmo; não se pode sair tutelando a torto e a direito, bem jurídico assim, só porque pensa que tem que tutelar.

Desculpem estar falando algo que possa ofender alguém, especialmente em Brasília, mas o nosso Direito Penal chegou ao ponto de ser movido a *Fantástico*: se foi veiculada reportagem investigativa no domingo, na terça-feira, já há projeto de lei sobre aquela matéria. O deputado não quer perder a oportunidade de dizer, no *Jornal Nacional* da quarta-feira, que tem um projeto de lei para acabar com aquele tipo de conduta.

Isso é um absurdo, porque, dessa tal forma, rompe-se com o sistema, e começa-se a legiferar a torto e a direito, achando-se que é na Justiça Criminal que os problemas serão resolvidos. É fácil resolver o problema criando leis, facílimo, porque tem delegado, tem Polícia Militar, tem Polícia Federal, tem perito, tem promotor, tem juiz criminal, tem o desembargador, tem o ministro. Por exemplo, diz-se que problema

ambiental é de responsabilidade do juiz criminal. Mas não é. O juiz ambiental é um dos responsáveis pelo problema; aliás, o último. O problema é do Instituto do Meio Ambiente e Recursos Naturais Renováveis (IBAMA) ou da Secretaria Municipal do Meio Ambiente. Não transfiramos para o Direito penal aquilo que não lhe é próprio, como se o juiz de direito fosse um mágico que, com uma varinha de condão, resolvesse os problemas do mundo. O juiz fica com o problema na sua mesa, concluso. Porque criaram um sistema de leis penais para tratar de matérias que não lhe caberiam.

Digo isso porque vivemos o Direito do Terceiro Movimento, do Quarto Movimento, do Direito Penal de Quarta Velocidade, de Terceira Velocidade. Não é isso que estão falando?

A classificação aqui apresentada tem muito a ver com a ideia de modernidade e de Direito Penal. O Direito tradicional, desde sempre, defendeu – desde a época da ordália, dos juízos de Deus – trata de bens jurídicos individuais como honra, vida, patrimônio. Com o passar do tempo, surgem alguns crimes coletivos. O Código Penal de 1940 já se referia a incêndio e a inundação, por exemplo. Mas aparece a tal da natureza difusa, o que começa a complicar.

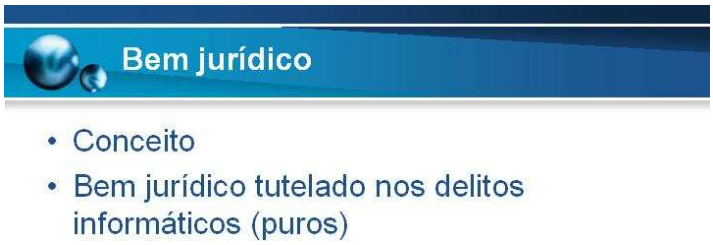
Cito um exemplo: estávamos, eu e minha filha, Fernanda, assistindo a um filme, e o enredo do filme começa a complicar. Lá pelas tantas, minha filha pergunta: "– Quem é do bem e quem é do mal?" Respondi: "– Do mal é aquele ali." E ela indaga: "– Mas por que, se ele era bonzinho e agora ficou do mal?" É a tal da natureza difusa.

O bem jurídico difuso é ofendido muitas vezes, aliás, na maioria das vezes, por pessoas do tal "colarinho branco" – Edwin Sutherland abordava esse tema na década de cinquenta. Tem promotor que chega no interior, acabou de passar no concurso, e está querendo muito entrar com uma ação civil pública contra alguém; e o juiz também, pois precisa dar uma liminar para fechar aquele negócio. Na cidade, encontram uma única empresa – cidade do interior só tem a prefeitura que emprega, a

Secretaria da Educação, que emprega professor, e alguma fábrica que, eventualmente, polua – não que eu seja contra, sou amigo do Ministro Hermann Benjamim, era Coordenador de Centro de Apoio com S. Exa., que respira Direito Ambiental – não posso falar isso sem correr riscos –, mas que não pode fechar, porque, se tal ocorrer, a outra metade da cidade fica sem emprego. Então, começamos a construir. Daí vem a tal da natureza difusa, aquela que se refere a uma sociedade na totalidade, que, como o bem coletivo, não tem disponibilidade, tem uma conflituosidade social, na qual mais ou menos não se consegue explicar quem é do bem e quem é do mal, pois, ao mesmo tempo que a empresa sonega e polui, dá emprego; e, ao mesmo tempo que vende produto fora da tabela, fomenta a economia local.

E aí, o que fazemos com a empresa? Cadeia? Fechamos? Não, temos os tais termos de ajustamento de conduta, para que não sejamos tão rigorosos com a aplicação da lei, porque, a rigor, não se pode tergiversar, mas se tergiversa porque a lei permite. A empresa compromete-se a diminuir a poluição, instalando os filtros em dez anos. Daqui a pouco para, mas enquanto não chegar... O termo é homologado no crime, transação penal, suspensão condicional do processo. O projeto de lei do Código de Processo Penal diz que haverá transação para tudo. Barganha. *Plea bargaining,* como falam os americanos.

Então, diminui o custo. Isso é mercado, é mediação, é negociação. E, no Direito da **ultima ratio**, está começando a ter isso.

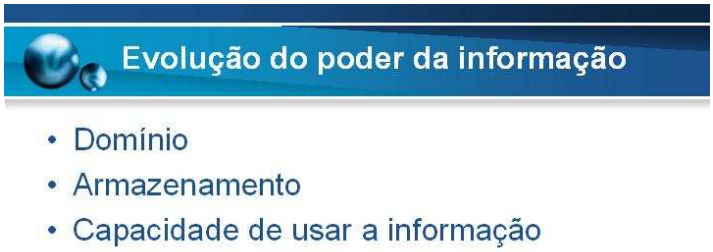


O bem jurídico que existe nesses crimes puros tem o nome de segurança informática. Ao criarmos um sistema de leis penais que vise a proteger o sistema, a rede, e a transformá-la em algo útil – se não transformarmos a rede em ambiente seguro, apenas vamos utilizá-la para brincar com joguinhos e baixar fotos do Frei Damião, do Padre Cícero, do Papa – e seguro, teremos que construir um sistema de legislação penal que garanta a integridade da informação. A não ser que queiramos disponibilizar a informação – como fiz agora com a minha tese – sem restrições, apenas citando a fonte.

Integridade, disponibilidade e confidencialidade são os elementos que constituem o bem jurídico segurança informática, que aparecerá como um bem jurídico permanente. Fui criticado na Banca pelo Dr. Miguel Reale Júnior, que indagou: "Como bem jurídico segurança informática?" A quem respondi: "Doutor, e nos crimes puros, o que visamos proteger? Não é só indenidade da eleição, é a segurança do sistema, especialmente nos crimes previstos no projeto de lei do Senador Eduardo Azeredo. Ou não queremos uma internet segura?

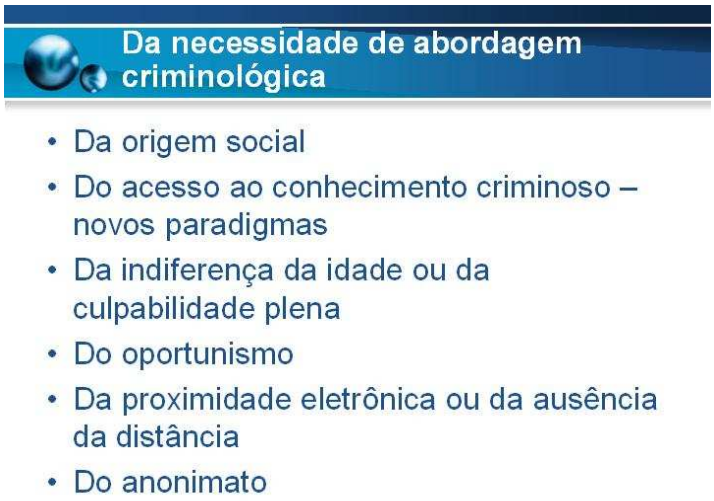
Quando perguntamos quem compra na internet, todos dizem que sim. Ao perguntarmos quem usa o cartão de crédito na internet, poucos

respondem que sim. Se perguntarmos quem compra, emite boleto, informa o código de barras, utiliza o *home banking*, abre sua conta de banco – porque acredita, confia no *site* – e compra, todos respondem sim, porque se sentem mais seguros dessa forma, ou seja, estão buscando segurança informática.



Essa é a história. Para quê? Para poder dominar, armazenar e ter a capacidade de usar a informação. Na década de setenta e oitenta, os governos militares diziam que informação é poder. Hoje temos que mudar esse lema, porque todos tem acesso à informação. Se quiser entrar no *Google*, tem informação do que quiser, der um passarinho que mora na Tanzânia, amarelo, verde ou azul. Agora, o que vai fazer com isso eu não sei. Essa é a questão. Não é só ter a informação, é a capacidade de usar essa informação. Esse é o xis da questão. O quanto eu sou o bom na coisa, de usar o que tenho acesso, porque todo mundo tem acesso ao Google. Tem até um neologismo, no novo dicionário vai ter "Googlar". Já estão usando isso. Todo mundo tem esse acesso.

Neste momento, começamos a refletir sobre a necessidade, sim, de um tratamento jurídico penal especifico para o tema.



Discursamos até agora sobre história, conceito, classificação e bem jurídico, e falaremos rapidamente de protagonistas, de autores, assim como, discorremos sobre o bem jurídico difuso de um novo ator, para entendermos o tema.

Na internet, a criminologia já se volta a realizar estudos específicos com relação ao autor do crime. O Delegado Mauro Marcelo Lins e Silva, dizia que dá para fazer um biótipo do adolescente que comete as infrações digitais, os atos infracionais, para sermos puristas, nos termos do art. 103 do Estatuto da Criança e do Adolescente (ECA). Diz o Delegado que a pessoa é muito branca, ou muito pálido, se afrodescendente, bem desbotado, e obeso, porque não sai da frente do computador, não toma sol e come porcaria o dia inteiro.

Não sei se está certo, mas o fato é que temos, dentro de uma visão criminológica – não concordo com o Mauro Marcelo –, temos um criminoso cuja origem social é diferenciada. Se bem que com as *lan houses* começamos a ter o acesso facilitado. Mas a prática de crimes

puros, próprios, com alta tecnologia, não custa barato. É possível chegar até um ponto, e depois disso é preciso entrar com alta tecnologia. Muitas vezes nos deparamos, nesses casos, não com aquele criminoso tradicional, aquele que a Polícia Militar não consegue precisar, mas que, na prática, é definido como "atitude suspeita".

Outro dia fomos falar sobre a visão do Ministério Público sobre abordagem policial. Naquele mesmo dia pela manhã, fomos aplicar prova, era novembro, ano passado, e estava muito calor. Havia um menino, aluno meu, péssimo, com uma jaqueta para 10°C. Olhei para o garoto e imaginei o que estaria acontecendo: atitude suspeita. Neste momento, pedi para ver a sua jaqueta, que, conforme verifiquei, tinha "cola" dentro. Não consigo descrever o que é atitude suspeita, mas a Polícia Militar consegue. Não dá para escrever sobre isso.

Origem social. Não existe *hacker* dentro de favela. O *hacker* é alguém que tem acesso à tecnologia. Aliás, outro dado desse aspecto criminológico: o acesso ao conhecimento criminoso, novos paradigmas. Como apareceu na nossa cultura a dogmática das aulas? Vamos à escola, o professor fala, fala, fala. Vamos embora, chegamos em casa, fazemos a lição e estudamos. Como funciona na internet? Entramos no *Google*, acessamos uma palavra-chave, vamos a uma página e, se não gostamos, voltamos para o *Google*. Erro e acerto, até encontrar algo de que gostamos. Poxa, isso é legal! Vamos ao *site* da *Wikipedia*, vamos a outro lugar, vamos ver de outro jeito, vamos fazer a pesquisa. O Professor de Filosofia Pierre Lévy, da Universidade de Paris, fala muito disso. E esse é o problema. É possível alfabetizar-se na rede, aprender a falar inglês; pode-se até fazer lição de inglês na rede, conversando com algum inglês: "*Hey*, estou tentando, ensina-me?" E alguém conversará com o interessado por meio da câmara. É diferente conhecer as coisas na rede, é completamente diferente, e não nos damos conta disso.

Antigamente, para procurar uma doutrina, íamos à biblioteca. Hoje, colocamos no site de busca , por exemplo, a expressão "erro de tipo", e

temos vários resultado sobre o assunto. Mais: "erro de proibição". É assim que estamos fazendo. Anteriormente, pegávamos e líamos o livrão da doutrina e íamos falar com o professor que não entendêramos a diferença entre erro de tipo e erro de proibição. Se o professor entendesse, explicava-nos.

Esse acesso ao conhecimento também se dá no crime. Como funcionava uma quadrilha? Os comparsas se reuniam veladamente e conversavam; ou faziam parte do mesmo bairro, ou haviam sido presos na mesma penitenciária. Agora, a quadrilha da rede atua de tal forma que alguns integrantes nunca se viram e são parceiros de crime. Paraopebas, no Pará, é um lugar com muita conduta criminosa nessa área. Comete-se crime contra o patrimônio, em concurso de pessoas, com quem nunca se viu; são parceiros de crime e nunca se deram as mãos. O acesso a esse conhecimento criminoso se deu por esse instrumento holístico que é a rede, a internet.

A indiferença da idade ou da culpabilidade plena. Hoje o crime organizado está cooptando. No mercado não existem profissionais gabaritados. É como o crime. Hoje o PCC, para lavar dinheiro, usa de *home banking*, e precisa de pessoas para serem os "laranjas" na rede. E quem faz o programa, quem faz a coisa? Nosso perito falará disso. Como acontece? E aí eles vão ao ninho, às escolas de Informática. Lamento dizer isso, mas há quadrilhas que pagam cursos para seus partícipes, e não só de Informática, de Direito também.

Podemos dizer que o oportunismo também é uma das formas que fomentam a criminalidade na internet. E vou dizer da minha instituição. Tivemos um concurso do Ministério Público, para Oficial de Promotoria, com 45 mil inscritos. Trabalhei no caso por designação do Procurador-Geral. Um dia recebi um rapaz na minha sala, terça ou quarta-feira, o concurso havia sido no domingo, dizendo, que havia tido acesso às questões de literatura e de português da prova. Perguntei a ele por que

não avisara antes, pois cancelaríamos o concurso. O fato é que não passou e foi lá falar isso.

Começamos a investigar, e vejam o que aconteceu. A professora de português e literatura contratada para fazer as questões partilhava o computador com a filha, que baixava músicas pelo *Kazaa*, que é um programa de baixar música. Quem mexe com isso sabe o que estou falando. É possível entrar na máquina de outra pessoa pela janela do *Kazaa*. Entraram, foram na parte da mãe, e pegaram as questões, dá até para fazer o rastreamento por palavra, por arquivo. Publicaram as informações num blog sem identificação, e na sexta-feira muita gente já sabia quais as questões que caíram no concurso do Ministério Público do Estado de São Paulo no domingo. Puro oportunismo.

Quem denunciaremos neste caso se não descobrimos quem invadiu? Vamos denunciar a professora por divulgação de segredo com dolo eventual? Afinal de contas ela assumiu o risco de produzir resultado ao partilhar computador com a filha? É ser hermeneuta demais, é estender demais a norma penal. Não dá. O concurso foi anulado e o caso foi arquivado. No segundo concurso, não tínhamos 30 mil inscritos. Ou seja, perdemos 15 mil candidatos, bons profissionais, que decidiram não fazer esse concurso. Ninguém foi punido. Puro oportunismo, com receita de bolo. Não precisa ser nenhum *hacker* ou *cracker* inteligente para fazer isso.

O que é receita de bolo? Vá aos grupos de discussão de *hacker* e vai conseguir um monte de coisas.

Outra coisa que entendemos que fomenta a criminalidade é a proximidade eletrônica ou a ausência de distância. Muita gente deixa de cometer crime por medo de a vítima reagir, por receio. O ladrão é alguém que tem receio de assaltar. Estatisticamente as mulheres são mais assaltadas que os homens, porque o ladrão tem mais coragem de assaltar as mulheres. A questão é física. Na internet não há receio nenhum, pois a

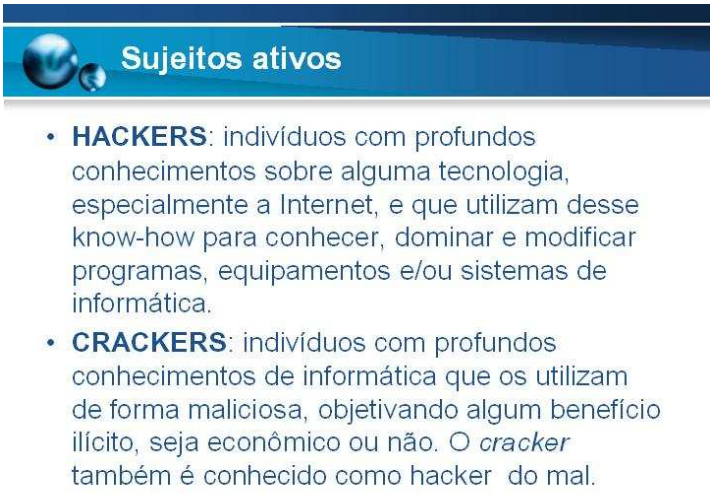
vítima não irá reagir, não existe legítima defesa digital. A Advogada Patrícia Peck sustenta que sim, e achamos que não.

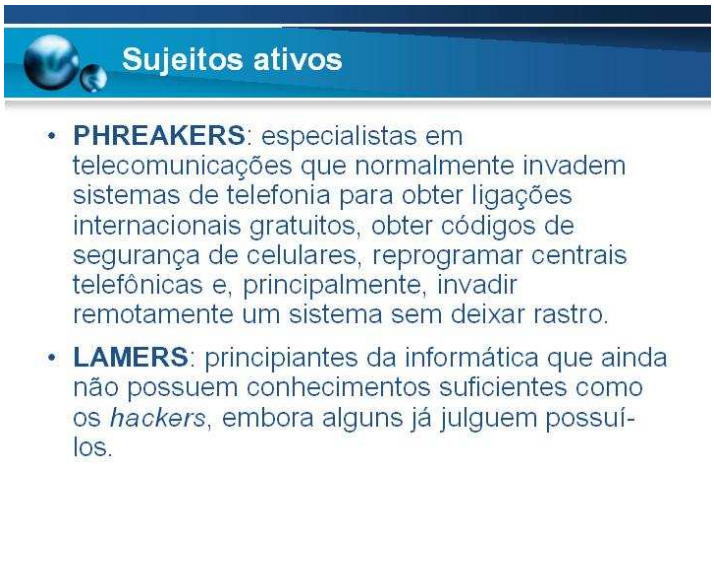
Para mim, é caso de inexigibilidade de outra conduta, o que exclui culpabilidade. Escrevemos sobre isso: a Advogada defendendo tratar-se de legítima defesa e nós de típico e de antijurídico, mas que não atribuindo culpa. Ela dizendo ser lícito, por hipótese, uma empresa invadida ir a quem a invadiu e pegar de volta o que lhe foi subtraído e destruí-lo. Para mim trata-se de exercício arbitrário das próprias razões. Só não é por conta da inexigibilidade de outra conduta. Nosso perito não vai na hora. Não dá, só chegamos muito depois. Então, sustentamos essa diferença. Mas sobre isso podemos responder durante as questões.

A inexistência de distância faz com que se fomente fortemente a prática criminosa.

E, por fim, o anonimato. Nem vou falar do anonimato, porque isso é um dos elementos dos aspectos criminológicos que estão aí. Mas é o anonimato paradoxal. Nosso perito vai falar dos rastreamentos. Se tenho um carro furtado, num cruzamento de duas ruas; se não tiver o Sistema de Posicionamento Global (GPS), nem sei para que lado o carro foi; na internet, não, tem o sistema de IP, tem os registros etc. Não falo do anonimato propriamente dito, falo do anonimato da pessoa que acessa a máquina. Muitas vezes chegamos à maquina e não chegamos ao ser humano que acessou essa máquina. Esse é o grande desafio, hoje, da certificação digital, fazer o vínculo da pessoa humana com aquela máquina, com aquela informação colocada naquele momento, naquele instante.

E agora temos vários atores. Há quem diga que *hacker* não é criminoso, seria um curioso. Sou mais tendente a isso, todos somos hackers. O *cracker* é do mal. Um é o bom-bom, e o outro é o mau-mau. E não vou ter tempo de divagar, porque tem muita coisa ainda para apresentar.

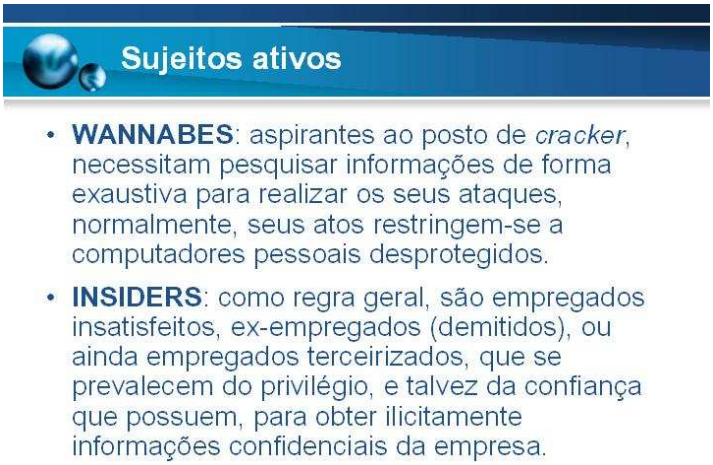




Os *freakers* são especialistas em comunicações que invadem sistemas de telefonia para obter ligações. Essa expressão, que antes da internet era usada para aqueles que faziam "gatos" de telefone, foi transferida para a internet.

Os *lamers* são os principiantes, que ainda não possuem conhecimento suficiente, como os *hackers*, embora alguns achem que possuem.

O *wannabe* é a mesma coisa, é uma contração do *i wanna be*, eu quero ser. Esse é bom de pegar, porque ele acha que é e deixa rastro fácil. Esse é fácil. Não que seja fácil, mas é menos difícil.



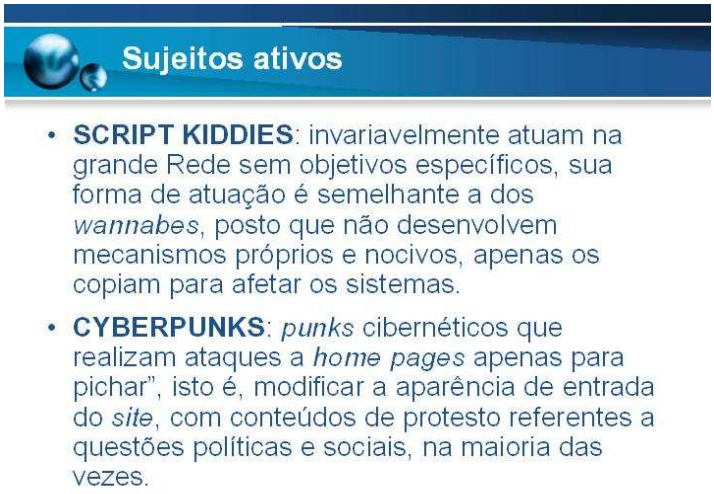
Os *insiders*, são os piores, porque são os do lado de dentro. Em regra, são empregados insatisfeitos, ex-empregados demitidos, ou, ainda, empregados terceirizados que se prevalecem do privilégio, talvez da confiança que possuem, para obter ilicitamente informações confidenciais da empresa.

O *Federal Bureau of Investigation* – FBI entende que 70% das ocorrências têm a ver com o *insider.* No jargão de polícia, diríamos "tem alguém que deu o pano", "tem alguém que deu o serviço", o vigilante do banco, a empregada doméstica; enfim, isso acontece. E na internet também, mas com muito mais frequência.

Aliás, uma vez estive em uma empresa, pessoas legais, olha, venha ver, implantamos um sistema. Vamos ver. Ao chegar, o Departamento de Informática, CPD, bacana, cheio de máquina nova etc. Aí comecei a olhar aqueles monitores, que ainda não eram de LCD, estava cheio de *post it* amarelinho. Ao olhar, eram as senhas das pessoas. Quer dizer, estavam todas as senhas no *post it.* Não dá. Aí não há quem consiga fazer proteção de ataque se tem isso. Passa uma pessoa lá e vai anotando todas as senhas, e depois, a pessoa que limpa – não que eu queira, vi uma pessoa lá em cima e nada contra –, mas o fato é que cria essa possibilidade.

Polícia investiga o lixo. Tive um colega, bom de serviço, lá em São Paulo, que, não conseguindo uma ordem judicial para entrar na casa de um dos investigados, vazou na imprensa que iria pedi-la. Ele foi para a

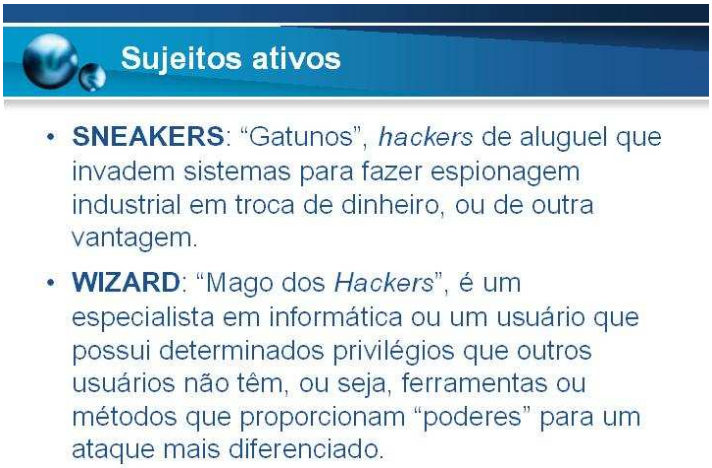
mídia e falou, olha, estamos entrando com pedido de busca e apreensão e tal e coisa. O investigado se desesperou de tal forma, que ele esperou passar o lixeiro, pegou uma caixa cheia de documentos e colocou no lixo. Aí já não era mais privacidade. Tinha uns agentes lá da Polícia de São Paulo, que pararam o caminhão e pegaram a prova para o promotor, sem a ordem judicial. Ou seja, isso se chama engenharia social. Com engenharia social, se consegue também, numa sacada dessas, obter a prova. Não sei nem porque falei isso. Bobagem.



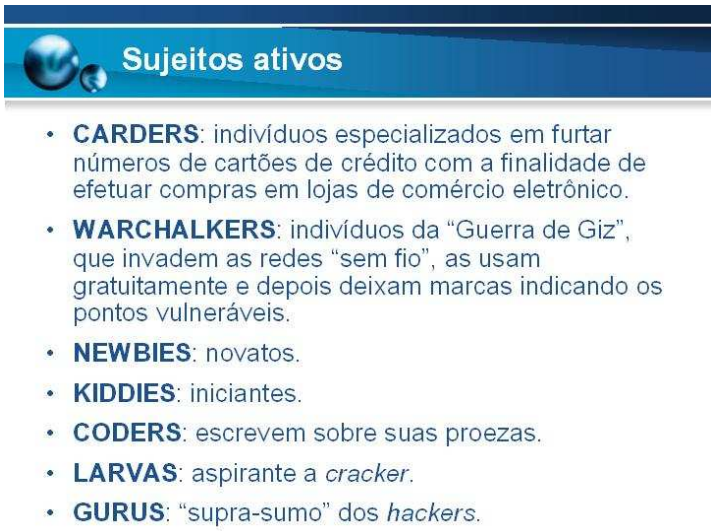
Os *script kiddies*, invariavelmente atuam na rede, sem objetivos específicos. É o pessoal que está passeando.

Cyber punks, que são os punks cibernéticos. Já picharam o *site* do Supremo Tribunal Federal, há muitos anos atrás. É dano virtual? Não, é conduta atípica. Crime contra a honra do Supremo Tribunal Federal?

Sneakers, são os gatunos. Esses cobram. Temos conhecimento de que prestam serviços para quadrilhas especializadas, – eles têm a tecnologia – assim como outros alugam armas e coletes para assaltos a carro-forte. Tem gente que só aluga arma, e pega porcentagem do botim.



O mago dos *hackers* é o *wizard*, um especialista em informática, usuário que possui privilégios que outros não têm. Eles têm poderes. O mais famoso é o Kevin Mitnick, um *cracker* que foi pego pela polícia norte-americana, e hoje trabalha para essa polícia, é um consultor, até deu uma entrevista à Rede Globo. Hoje virou de lado.



Os *carders* – chamávamos de "cartãozeiros" – são especialistas em cartões.

Os *warchalkers* são aqueles que estão invadindo as redes *wireless*. A Elizabeth Sato, que hoje está no Departamento de Homicídios e Proteção à Pessoa (DHPP), é Delegada Titular do 78º Distrito Policial, localizado nos Jardins, na Avenida Paulista, conta que a Polícia Militar estava passando pela Alameda Santos e encontrou uma pessoa com um computador e uma latinha *pringles* de lado. A Polícia Militar abordou-o por atitude suspeita: quem anda com um computador e uma latinha *pringles* na rua? Descobriram que o indivíduo estava tendo acesso a algumas empresas ali na região da Paulista. Delegacia, foram para a delegacia. Apresentaram a ocorrência, chamaram o pessoal do Instituto de Criminalística. Olha, ele estava acessando a empresa tal, e chamaram o representante comercial. Aí delegada me liga e diz, olha, Rossini, pegamos uma pessoa em flagrante.

Qual é a conduta? Invasão de domicílio? Que conduta é? Crime contra a propriedade intelectual da empresa? Não é nada. Foi feito um Boletim de Ocorrências, de preservação de direitos, para a pessoa poder impetrar uma ação de indenização contra ele. E ele ainda brincou: olha, tchau! A Delegada ainda quis requisitar a máquina para fazer perícia, e ele disse, olha, não tem conduta típica. Veio um advogado e orientou, e aí ele

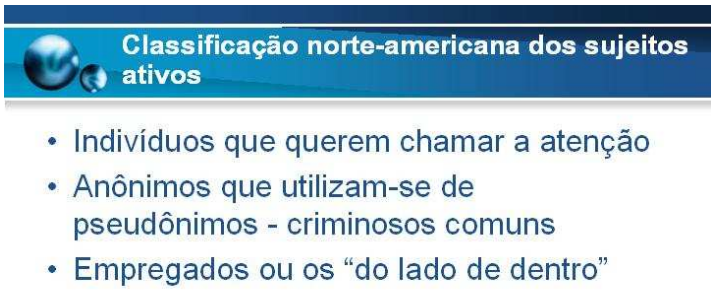
foi embora. Ainda brincou: "– Olha, vou emitir uma fatura, porque estou fazendo consultoria de graça para vocês. O sistema de defesa da sua empresa está uma porcaria, qualquer um entra. Eu entrei lá da rua, com um sistema de *wireless*."

Não tem conduta atípica.

Chama-se "Guerra de Giz" porque, nos Estados Unidos, os *warchalkers* ainda faziam o favor de marcar o chão para dizer que naquele lugar ali estava fácil de entrar, havia buracos nas redes locais.

Há também os *newbies,* que são os novatos, os *kiddies*, os *larwas*, etc.

Classificação do FBI: indivíduos que querem chamar a atenção, anônimos, empregados ou os "do lado de dentro". Caberia acrescentar os terroristas.



E propusemos outra classificação, à vista da categorização do crime apresentada anteriormente: são os sujeitos ativos próprios e os impróprios, puros ou impuros.

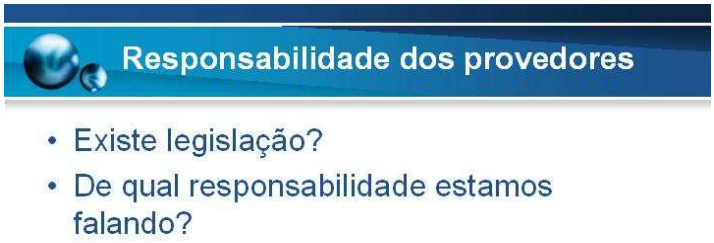
Impróprio é o sujeito que comete o estelionato em qualquer ambiente, fora, dentro da rede, no aeroporto, no banco, no Modo

de Transferência Assíncrono (ATM), em qualquer lugar.

Agora, existem profissionais que só atuam em rede, são os que atuam, por exemplo, com desvios de grandes valores por meio de *home banking*, são os invasores de sistemas, os criadores de vírus, criadores de programas maliciosos.

E queríamos falar rapidamente da casuística da responsabilidade dos provedores. E por que colocamos esse tópico próximo a "Sujeitos Ativos"?

Atentos a uma normativa do art. 12 da Convenção de Budapeste, por pensar, refletir acerca da possibilidade de um dia termos responsabilidade penal de provedor. O que atualmente não é possível por falta de amparo constitucional.

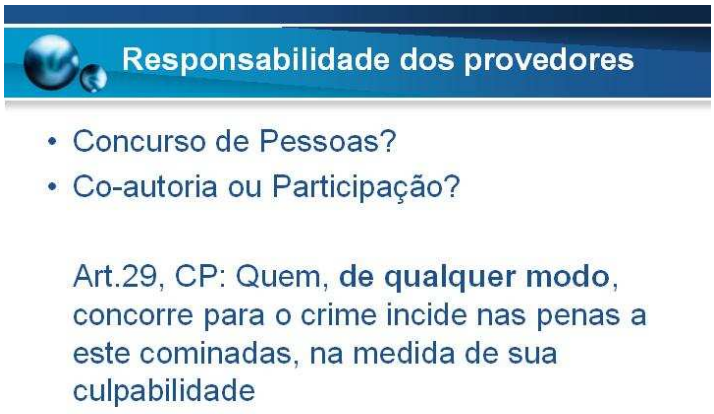


Todos aqui devem saber que, para atribuirmos responsabilidade penal à pessoa jurídica, como consta do art. 3º da Lei nº 9.605, que trata de crime ambiental, houve a necessidade de, no art. 225, § 4º, que joga a responsabilidade... Há uma dúvida, há quem diga que não.

O art. 175 da Constituição diz da responsabilidade penal da pessoa jurídica nos crimes contra o Sistema Financeiro, contra as relações de consumo. Só que, passados 22 anos, da promulgação da Constituição, não

se teve a regulamentação, por exemplo, da responsabilidade penal dos bancos, e pouco provavelmente haverá, por razões óbvias. Sabemos como o sistema funciona.

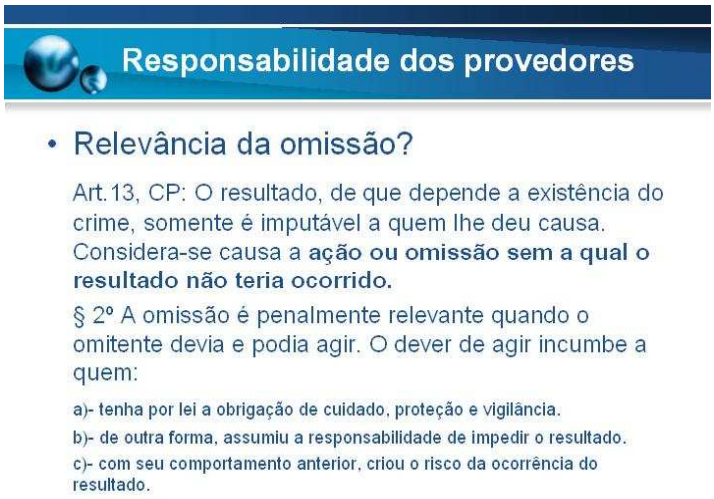
Mas não dá para se falar em responsabilidade penal do provedor à míngua de amparo constitucional, simplesmente porque, em 1988, não havia *internet* no Brasil. Não dava para antever... Então, para que ocorra essa responsabilidade, devemos, antes, alterar a Carta Constitucional.



Mas dá para pensar, dá para refletir sobre responsabilidade penal do provedor? Do ser humano sim, da empresa, não. Mas, de qual responsabilidade? Temos dois caminhos. Proponho a ideia de um debate sobre esses dois caminhos. Evidentemente que o primeiro deles é a participação. Claus Roxin, representante da Teoria Alemã. tem um livro enorme abordando a Teoria do Domínio do Fato. Sabem por que tiveram que criar a Teoria do Domínio do Fato? Porque não tem o 29 como o nosso. O conceito deles é muito mais ligado à coautoria do que à participação. A reforma de 1984, do nosso Código Penal, trouxe para o ordenamento jurídico brasileiro, que a norma seja completada pelo intérprete.

Vou trazer aí o caso do Glauco. O menino que levou o carro, teve participação ou não teve? Quais as formas de participação? Moral e material, instigue, induza ou auxilie. Instigação ou induzimento é formal, e a outra é material, como oferecer a arma, etc. Quem construiu a participação desse rapaz? O delegado. Quem eventualmente vai construir a participação dele? O promotor e o juiz, se receber a denúncia. A norma é aberta, extremamente aberta, e por ser aberta é que pode ser

imputada, há como se imputar participação ao ser humano que trabalha num provedor. Só que tem alguns requisitos, tem que ter dolo. A participação tem requisitos, como número superior a uma pessoa, porque senão não tem como ter. Mas o que pega na participação é que não tem participação culposa. Só tem participação dolosa. Pode até ter coautoria culposa. Vamos jogar uma tábua, lá de cima do prédio até embaixo. Os dois estão com culpa, foram imprudentes. Agora, não dá para ter participação culposa. E não tendo participação culposa, tem que encontrar na investigação o dolo do provedor. E aí o "bicho pega".



O outro caminho, que considero mais fácil de se trilhar para alcançar, Professor Ulysses, os provedores, é a tal da relevância da omissão. Relevância penal da omissão. Transforma, por lei ou por contrato, ou por outro ato o provedor em garantidor, e dele se exige que haja. Aliás, outro problema para se estudar, no Brasil, é a tal da imputação objetiva, é o art. 13. Todo mundo tentou construir, há uns cinco ou seis anos atrás. Quem estudou Direito Penal recentemente sabe o esforço que é para entender a tal da imputação. Incremento do risco. Que coisa é essa de incremento do risco? Estou pensando ainda com a regra de três do nexo causal, do art. 13, caput. E o que ele diz é isso, o resultado de que depende a existência do crime somente é imputável a quem lhe deu causa. Perfeito. Essa é a regra de três. O resultado depende de que depende a existência do crime, ou sejas, nos crimes materiais, não nos crimes formais, porque nos crimes formais não tem resultado, somente é imputado a quem lhe deu causa. É óbvio. Só que a causa é aquela ação ou omissão sem a qual o resultado

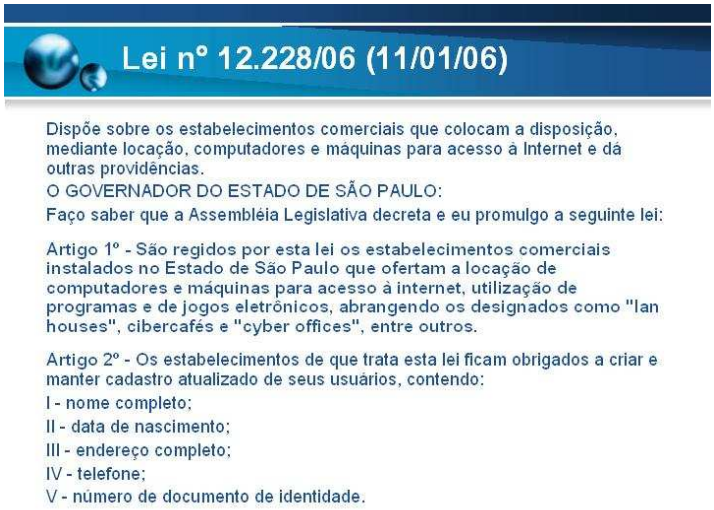
não teria ocorrido. É como disse o **sine qua non**, que já estudamos bastante, na cátedra.

Mas aí falam, ação, tudo bem; e a omissão? A omissão, no parágrafo 2º, é penalmente relevante quando quem omite devia e podia agir. É a figura do garante. Temos essa visão. É uma solução que um promotor dá. Se for falar com o advogado da Google, ele vai me rechaçar. Ninguém mandou convidar só promotor para falar... Na próxima chamem um advogado, minha boca está torta e me orgulho disso. Não fiz concurso para magistrado, não vou pelo quinto constitucional, meu "babado" é ser promotor de justiça, adoro.

Regra de três, o dever de agir. Poder agir. Poder agir é a história do bombeiro, ele tem o dever de agir, mas se estiver pegando fogo ele não tem que entrar senão vai morrer também. Não estamos discutindo essa possibilidade de agir, e o provedor pode agir. O dever de agir incumbe a quem? Aí vem a omissão, quando tenha por lei a obrigação de cuidado, proteção ou vigilância. A lei determina, o art. 241 do ECA determina. O provedor é garantidor.

De outra forma assumiu a responsabilidade de impedir o resultado – contrato. O legislador não quis dizer contrato. Se alguém aqui leu o contrato que fez com o provedor, ganha um copo de água, porque ninguém lê. Ninguém lê, mas tem, e tem que eles não se responsabilizam. É nítido isso.

E comportamento anterior criou o risco da ocorrência do resultado. Aí tem o incremento do risco. O tal do incremento do risco, que a doutrina alemã fala bastante, está aqui no nosso código. Não precisamos viajar para longe, tem muita gente boa que fala aqui no Brasil.



Lei nº 12.228/06 (11/01/06)

Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências.

O GOVERNADOR DO ESTADO DE SÃO PAULO:

Faço saber que a Assembléia Legislativa decreta e eu promulgo a seguinte lei:

Artigo 1º - São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como "lan houses", cibercafés e "cyber offices", entre outros.

Artigo 2º - Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

I - nome completo;

II - data de nascimento;

III - endereço completo;

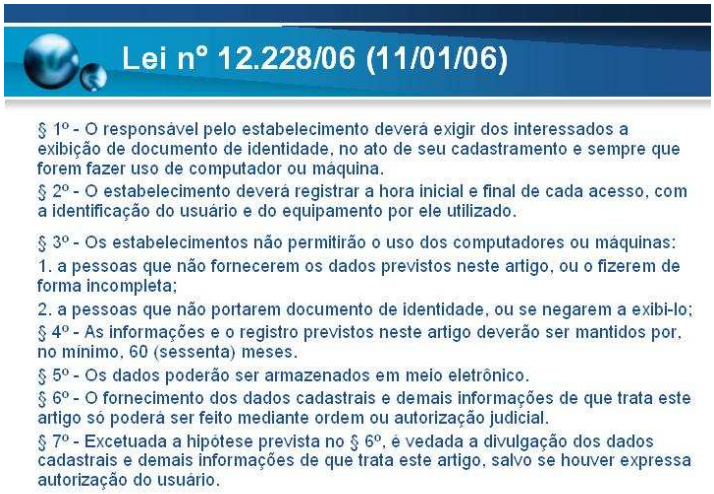
IV - telefone;

V - número de documento de identidade.

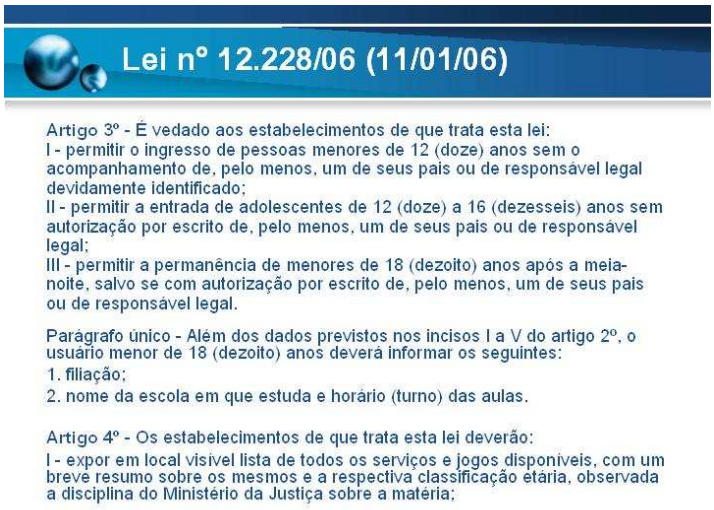
Olhem como São Paulo tentou resolver o problema, e outros estados também: criando a figura do garante, para o provedor chamado *lan house*, para o provedor chamado cyber café. E dá para fazer isso com legislação estadual? Dá, porque quem regulamenta o exercício do comércio no Estado de São Paulo é a Junta Comercial. Aliás, a própria Constituição defere essa possibilidade ao Estado federado. E aí não se fala em interferência da União.

Vejam: "O Governador, [no uso das atribuições] [...] são regidos por essa lei, os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como *lan houses*, cybercafés e *cyber offices*, entre outros" [são os provedores de acesso e os provedores de serviços]. "Os estabelecimentos de que tratam essa lei ficam obrigados a criar e a manter cadastro atualizado de seus usuários, contendo nome completo, data de nascimento, endereço completo, telefone, número de documento de identidade".

Pena que o legislador estadual não teve a cautela de colocar um inciso VI, dizendo "foto", que todo computador tem hoje a maquininha, a *web cam*; podia falar isso também. Exige tudo e tira uma foto, porque a pessoa pode usar documento falso. Esse é o pé de barro que a legislação não abarcou. Mas está em tempo de mudar.



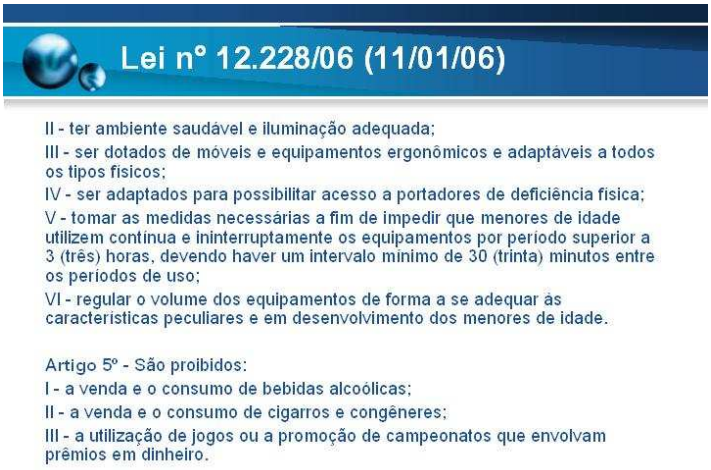
E aí vem: "o responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, nota do cadastramento sempre que forem fazer uso do computador ou máquina".



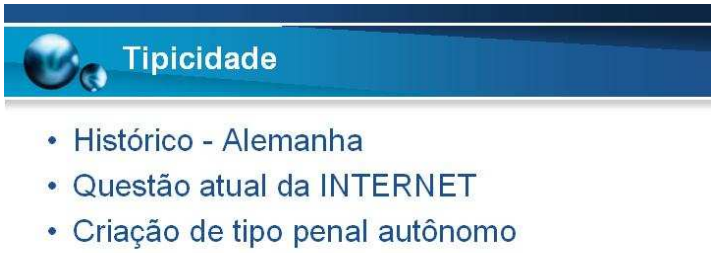
E aí vai a normativa, a regulamentação, inclusive com o uso de pessoas abaixo de doze anos, acima de doze anos. Vejam: "é vedado aos estabelecimentos de que trata esta lei:

I – permitir o ingresso de pessoas menores de doze anos sem o acompanhamento de pelo menos um dos pais ou responsável; de doze a dezesseis, sem autorização por escrito; e permitir menor de dezoito anos após a meia noite, salvo se com autorização por escrito dos pais ou responsável".

O fato é que com essa lei cria a figura do garante, a *lan house* vira garante. Tem gente sendo processada já, por responsabilidade civil decorrente disso, já temos julgados; ainda não tivemos *leading case* criminal para apresentarmos, porque em todas as oportunidades o provedor ofereceu os dados que tinha dos cadastros que por ali passaram.



Mas parece-me que é a única forma de responsabilizar penalmente o provedor, no direito brasileiro, que é a regra do art. 13, desde que tenha lei, como o art. 241 do Estatuto da Criança e do Adolescente, como lei estadual, ou como leis de outras naturezas, provimentos, portarias de ministérios etc., desde que respeitada a hierarquia das leis.



Agora vamos chegar na tipicidade, para irmos encaminhando para o fim. Em 1895, na Alemanha, instalaram a energia elétrica em Berlim. E aí teve um espertinho que fez o gato e pegou a energia elétrica. Vejam que na Alemanha também tem ladrão, tanto que têm Código Penal, não é privilégio do Brasil; aquele médico que fugiu de São Paulo foi para a Islândia, adorou ficar na cadeira lá, mas também tem cadeia na Islândia. Ou seja, o mal acompanha o homem. Eu brincava no júri, olha, como vamos conseguir resolver o problema da criminalidade,

se Jesus Cristo morreu entre dois ladrões, convenceu um só. Quer dizer, se Jesus Cristo obteve cinquenta por cento de reincidência, por que eu, um simples e falível mortal conseguiria. Nossa missão não é só recuperar o ser humano, é proteger o bem jurídico. Visão do promotor, da boca do promotor. Direito Penal tem suas missões, e na internet tem uma missão bonita, que é tentar resgatar a segurança informática. Não sei se vai dar.

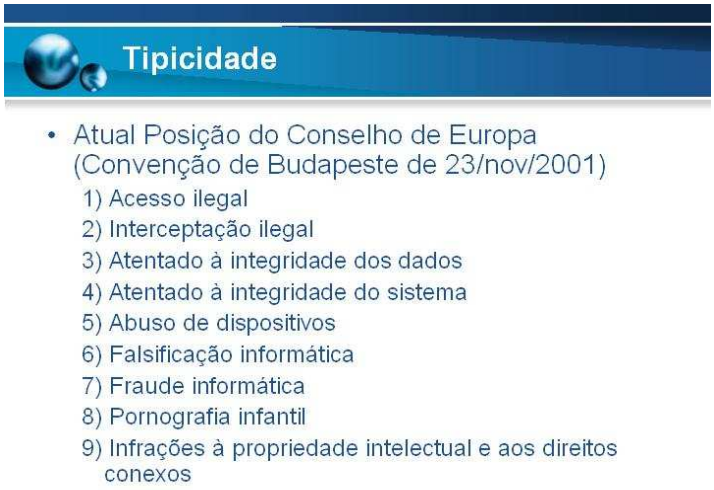
Essa pessoa pegou a energia elétrica, tungou, subtraiu a energia elétrica, prendem-no e o denunciaram por furto. Ele foi condenado, e chegou até o tribunal superior de lá. Disseram que a conduta era atípica, porque energia não poderia ser equiparada a coisa. Foi aí que nasceu o furto de energia elétrica. Nelson Hungria trouxe para o nosso Código esse exemplo do furto de energia elétrica: equipara-se a coisa à energia, ou qualquer outra energia, com valor econômico. Não é isso que está no art. 155, parágrafo 3º?

Energia é coisa? Qual outro exemplo de ficção? Ponha a mão na energia elétrica para ver. Toma choque, mas é passível de tutela do direito penal, porque por equiparação típica o legislador trouxe para o ordenamento jurídico a capacidade de alguém ser punido por fazer uso, por subtrair essa energia. Esse é o problema que estamos vivendo, ainda hoje, no Brasil, à míngua de todos os tipos, especialmente aqueles tipos que tratam da invasão e da destruição de dados à distância.

Conseguimos pegar por atacado, muitas vezes denunciamos na formação de quadrilha, para a prática de crime. É o estelionato. Mas a invasão por si, é aí que brinco sempre, hoje tenho uma lei no Brasil, fulano entra em minha casa, entra vai lá, olha minha esposa, meus livros, pega minhas coisas, mas não leva nada, vai embora. Invasão de domicilio. Se a pessoa fizer isso exatamente da mesma forma, mas virtualmente, não é nada, não é passível de tutela penal. Isso parece-me um absurdo.

Aliás, já que vivemos, na internet, esse paradoxo da liberdade versus punição, deixemos que os crimes digitais, as infrações penais

digitais sejam mediante ação penal pública condicionada, que pelo menos a pessoa manifeste o desejo de o estado atuar, vai lá e represente. Não por queixa, porque daí é "sacanagem", está tendo um problema sério com relação aos crimes contra a honra, porque ninguém entra com queixa-crime por crime contra a honra, nem no mundo físico, o que dirá na internet. Então, as pessoas suportam a ofensa e ficam quietas, ou fazem a retorção na rede: olha, chamou-me de ladrão, ele é isso também – e aí não tem pacificação.



A Convenção de Budapeste, que está no anexo, sugere a criação de nove tipos-padrão, para abarcar aquelas hipóteses ali previstas. Acesso ilegal. No Brasil tem acesso ilegal? Alguns têm, a Lei nº 9983, que criou o peculato eletrônico, fala do acesso; o próprio art. 72 da Lei nº 9.504 fala do acesso ilegal. Mas não estamos precisando só de ter lei para esses dois nichos, para tudo.

Tem interceptação ilegal? A Ada Pellegrini Grinover diz que não tem interceptação. Ela usa argumentos jurídicos, eu uso argumentos técnicos. Não dá para interceptar, aliás, o perito pode responder a essa pergunta, porque acho que não tem interceptação de dados, a interceptação, tem a coleta dos dados, mas interceptação enquanto os pacotes estão transitando, é de difícil caracterização. Eu não consigo. O que sustento, e depois coloco essa questão para responder. Eu penso que não se aplica a lei das interceptações aos *e-mails*, se aplica o art. 240 e 241 do Código de Processo Penal.

Como é o sistema de internet? Faço mensagem aqui, vai para o provedor, vai para o cyber espaço, cai no provedor da pessoa que quero,

o outro provedor e vai para a máquina da outra pessoa. Eu pego os pacotes enquanto está no cyber espaço? Não dá, só se tiver os pontos onde esses pacotes se juntam, quando saem ou quando entram.

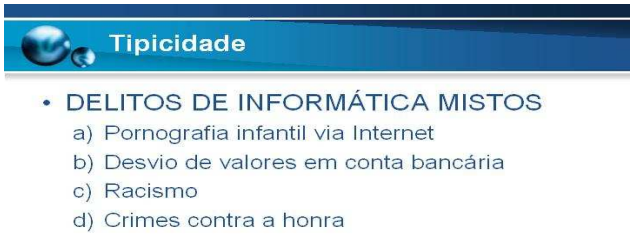
O dado é apreendido, não é interceptado. Estou tentando fazer uma consideração para tentar facilitar a nossa vida, não é para prejudicar, é para facilitar. Não interceptamos aquilo que é impossível, porque são pacotes. Como funciona? Pegamos a informação, apreendemos o dado. Quanto trabalho nos dados lá, não peço interceptação de *e-mails*, peço a busca do *e-mail*, no provedor de acesso de quem sai, de quem entra, o 240, e o juiz dá uma ordem. Pego a máquina, vou ao provedor e pego o dado. Aliás, tecnicamente é de difícil configuração, diferente de uma ligação, em que estamos ouvindo a pessoa conversar *on line;* aí é possível interceptar, pegar o que está em movimento. O dado não está em movimento, o dado está parado. É uma questão a se refletir, para facilitar a vida de quem investiga. É uma sugestão que trago.

Tem interceptação nesse caso, em que alguém se faz passar, mas a conduta é atípica. Essa é a interceptação, que seria a subtração de dados, no meu ponto de vista.

Atentado à integridade, tem no crime eleitoral. Integridade do sistema, também tem no eleitoral.

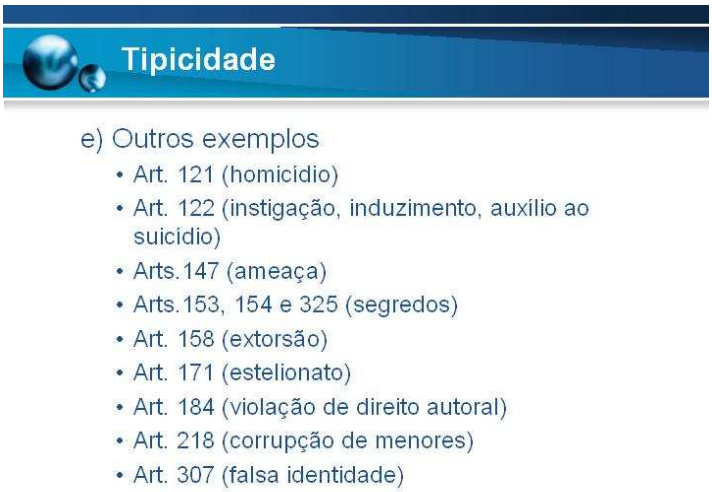
Abuso de dispositivos, ao que parece ao não tem.

Fraude informática é o estelionato; pornografia, já tem; e as infrações à propriedade intelectual, art. 184 e seguintes, que foram alterados recentemente.



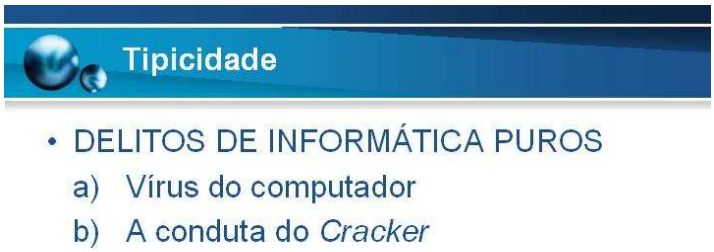
Mistos, são os exemplos que já citamos, como racismo, crimes contra a honra.

E aí trago toda a parte especial do Código, porque muitos crimes podem ser cometidos pela rede: homicídio, instigação, ameaças, segredos, distorção, estelionato; e da legislação à parte, cassino, pirâmide.



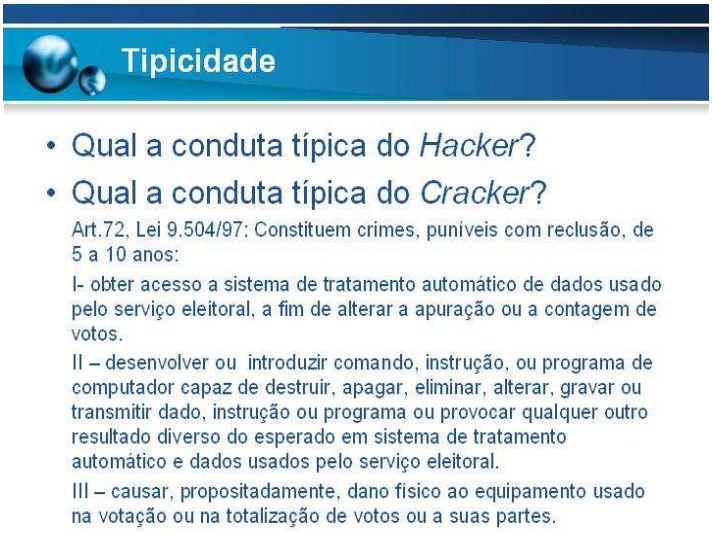
Rossini tem crime da lei de economia popular? Vou mostrar que tem. Interceptação telefônica, para quem entende desse jeito, *software*, art. 72 da Lei nº 9.504; a Lei nº 8666, que fala da licitação *on line,* pregão eletrônico que dá para pegar; a Lei nº 9983,

que trata dos crimes contra a Administração Pública; a Lei nº 10792; e a Lei nº 11829, que recentemente alterou o art. 142 do ECA.



Delitos puros. Conduta do *cracker*, o vírus.

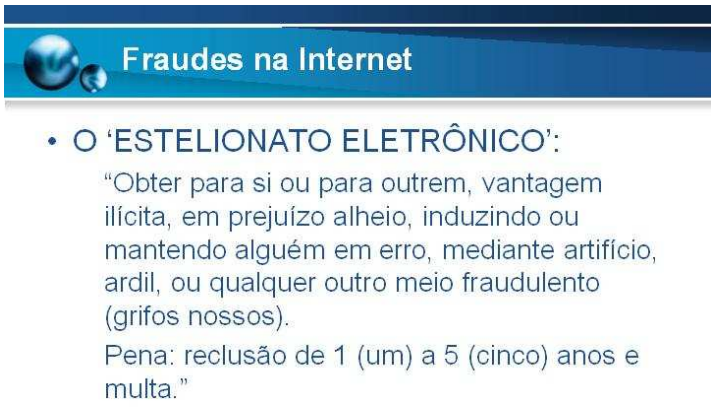
Art. 72: "constitui crimes puníveis com reclusão de 5 a 10 anos" Queria que essa sanha de preceitos secundários, de 5 a 10 anos, viesse para o homicídio culposo, de trânsito. Quer dizer que matamos uma pessoa na rua, dois anos de detenção; damos um chute na urna eletrônica no dia da eleição, cinco anos. Isso é uma loucura.



Cinco a dez anos, causar dano físico ao equipamento, crime eleitoral, crime misto. Eu saio correndo, atropelo alguém, dois anos; um é aberto, quando mato a pessoa; dou um chute na máquina eletrônica, semiaberto.

"Obter acesso a sistema de tratamento automático de dados, usado pelo serviço eleitoral, a fim de alterar a apuração; desenvolver ou introduzir comando, instrução ou programa" Aqui está o acesso e o vírus. São crimes puros, no ordenamento. A lei é de 1997. A lei tem treze anos.

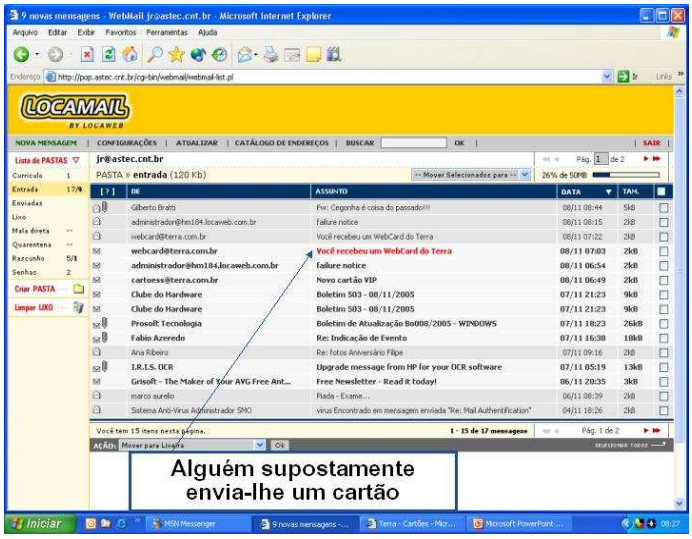
Não legislam porque não querem. Desculpem a crítica que faço, mas também não tenho que ser bonzinho.

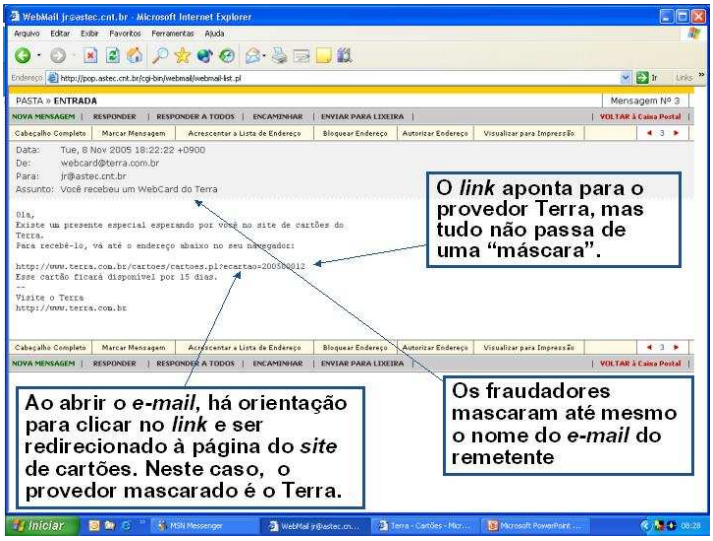


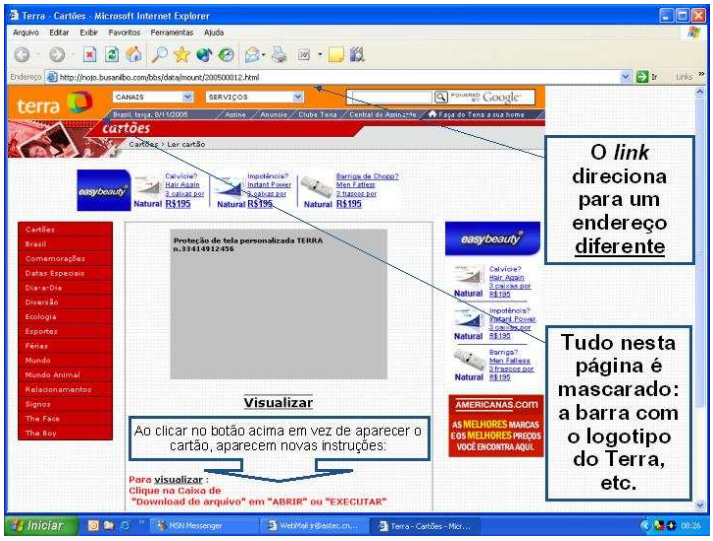
Estelionato eletrônico, coloco entre aspas. É o mesmo estelionato, porque também é um tipo aberto, ou qualquer outro meio fraudulento. Estamos usando o estelionato como um AAS, como aspirina, porque não tem outro jeito. Ou furto mediante fraude, porque a legislação não indica qual é a fraude, ou é o estelionato. Estão querendo criar o estelionato eletrônico. Já demos um parecer contrário. Não se sei vai passar. Estelionato é estelionato, fora ou dentro.

Isso aqui tem oito anos. Ao recebermos um cartão, hoje temos "duzentos" desses; ao abrir o link para o provedor Terra, mas não passa de uma máscara, uma isca. Ao clicar no link, ele é direcionado. Os fraudadores mascaram é isso, tudo aí é fraudulento. Não tem nada de Terra.

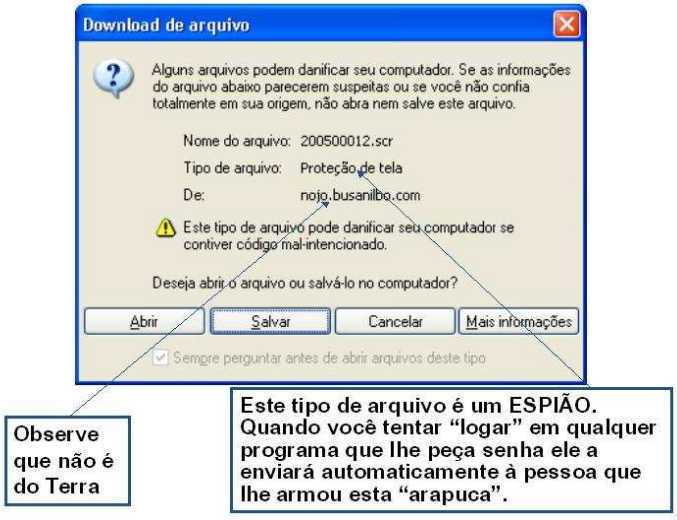
Exemplo de fraude na Internet via *e-mail*







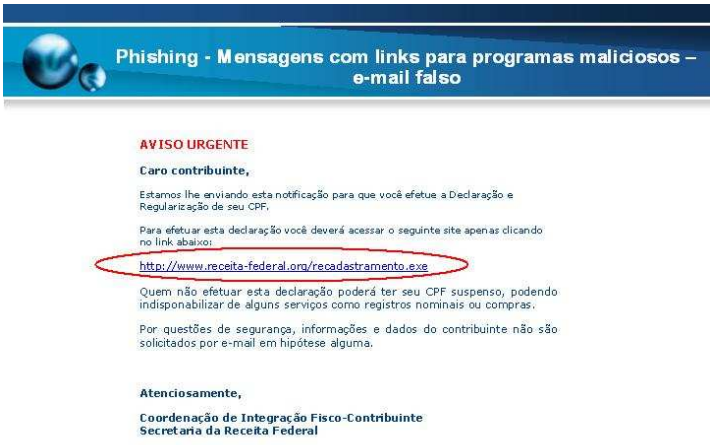
Quando se vai fazer a análise, o que é? É um protetor de tela, e foram dadas todas as informações.

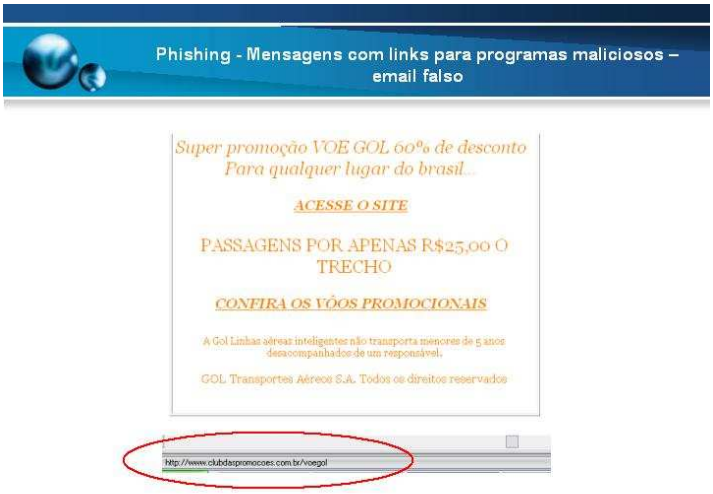


Aí está, certificado de depósito da Nigéria, tem quem compra na rede. E ai vão os exemplos.

Os *phishings, e-mails* falsos.

Cadastro da Receita Federal. Quem não recebeu um desses? É um arquivo da Receita Federal executável, é um *spyware*, um espião que vai entrar e ficar na sua máquina.



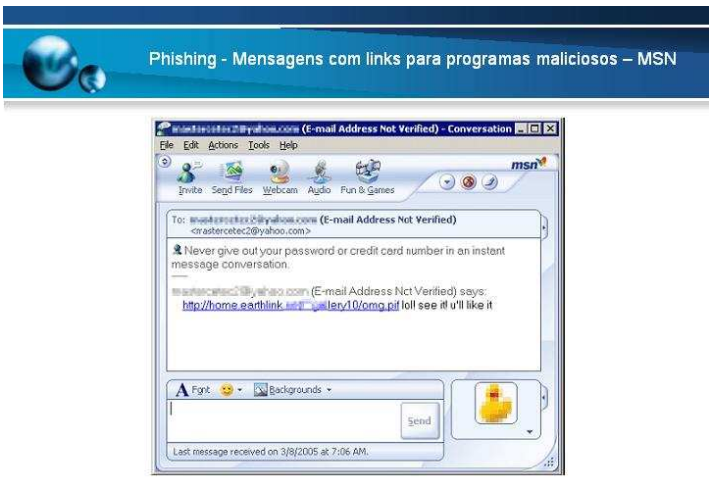


Acesse Gol, sessenta por cento de desconto. E ainda falamos daquele dolo recíproco. No estelionato só se consegue faturar em cima da vítima, porque ela tem muita ganância, e é aí onde a pessoa ganha dinheiro.

Gol, Tim, tudo falso.

Esse aí é engraçado: "Ejaculação precoce, 'nuca' mais..." Não fui em quem escreveu. Por que acessar uma coisa dessas? Está numa situação tão precária, tão ruim... E aí vou para a rede e acesso. Clico, é para "baixa o Manual". O internauta já está de moral tão baixa e aí acessa uma coisa dessas.

O *fishing* no MSN.



O *phishing* no Orkut[1].

Esse aqui, vou falar daqui a pouco.

[1] MSN e ORKUT → Rede de Serviços oferecidos pela Microsoft, para comunicação virtual

Bradesco, Banco do Brasil, Itaú...

Esse é de uma primariedade e ainda tem quem caia. E por que tem gente caindo? Porque está havendo, ao longo da nossa vida recente, a tal da inclusão digital. A inclusão digital é uma maravilha, para a sociedade e para o estelionatário, que o estelionatário pega os incautos que nunca acessaram a rede. Primeiro e-mail que ele recebe é para se recadastrar. Nunca falaram para ele não se recadastrar, aí coloca tudo que ele quer.

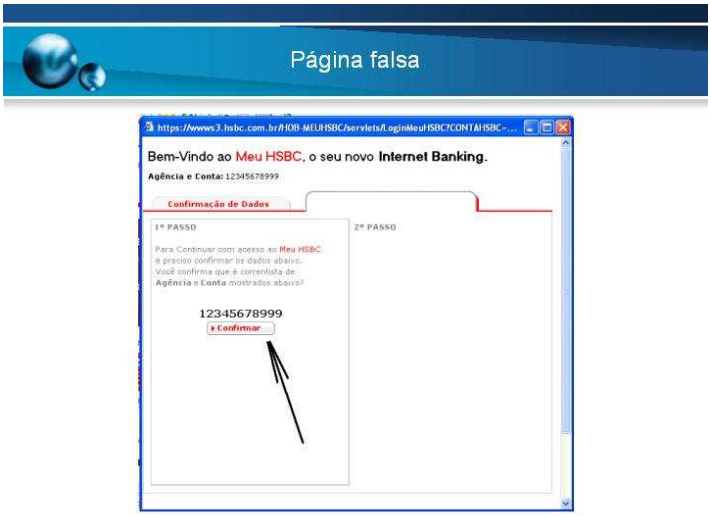
Olha esse aqui, é feito por *spam.* Manda cinco mil, e se um responder, bem, faturou. Não gastou nada para mandar os cinco mil *e-mails.*

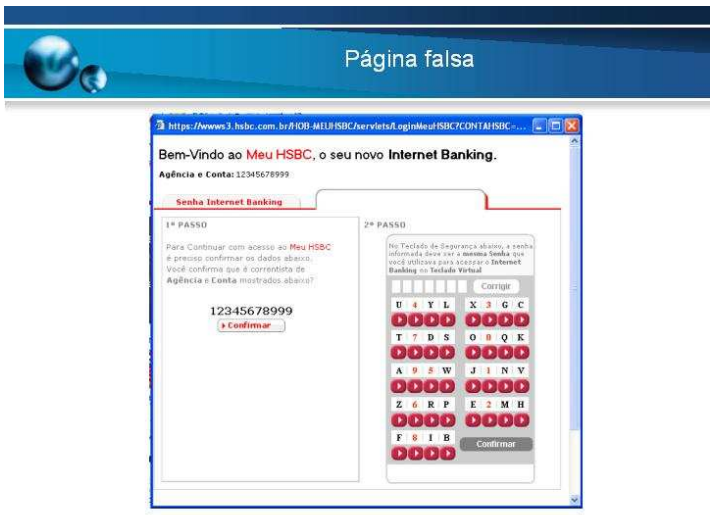
Esse aqui, a pessoa entra na página, tudo falso, e começa: "Consultas e transações. Esse é o seu selo digital, único e exclusivo que deve ser reconhecido a cada acesso". Confirma? Confirma.

Segundo passo: "Clique nos botões referentes aos sete dígitos de sua senha automática para acessar o *internet banking*". Vamos usar o teclado?

Percebe-se que começa a haver diferença de trato.

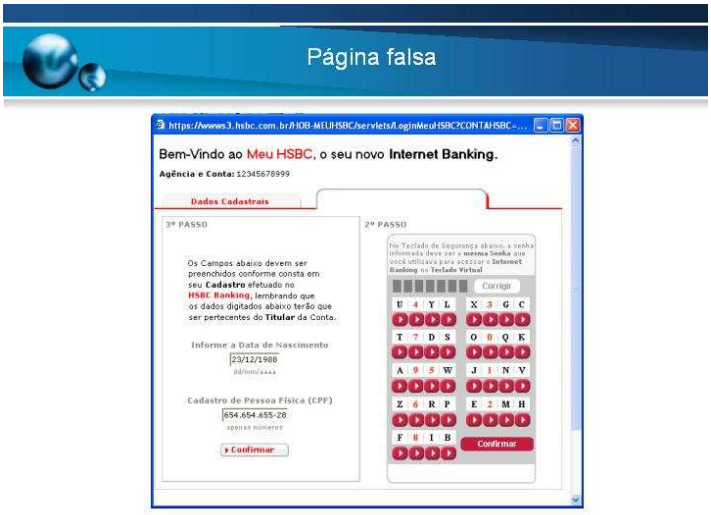
E aí vem, após o acesso, temos mais um passo: "Para continuar o acesso ao meu HSBC é preciso confirmar os dados abaixo. Confirma que é correntista da agência e A conta?" Confirma.

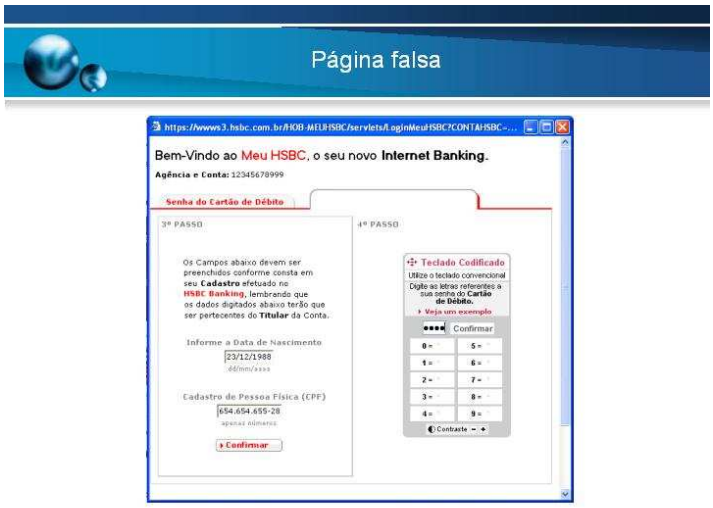




"No teclado de segurança abaixo, a senha informada deve ser a **mesma senha** [em negrito], que utiliza para acessar o *internet banking* e o teclado virtual".

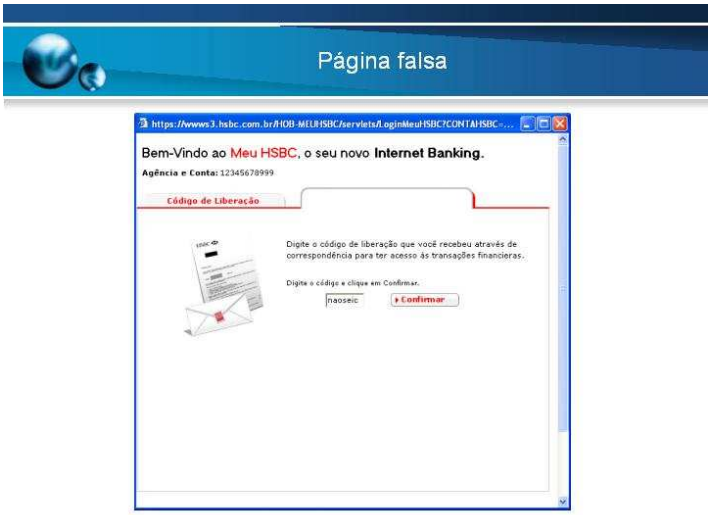
"Os campos abaixo devem ser preenchidos conforme consta em seu cadastro efetuado no HSBC *banking*, lembrando que os dados listados abaixo terão que ser pertencentes ao titular da conta. Informe a data do nascimento. Cadastro da Pessoa Física, CPF".

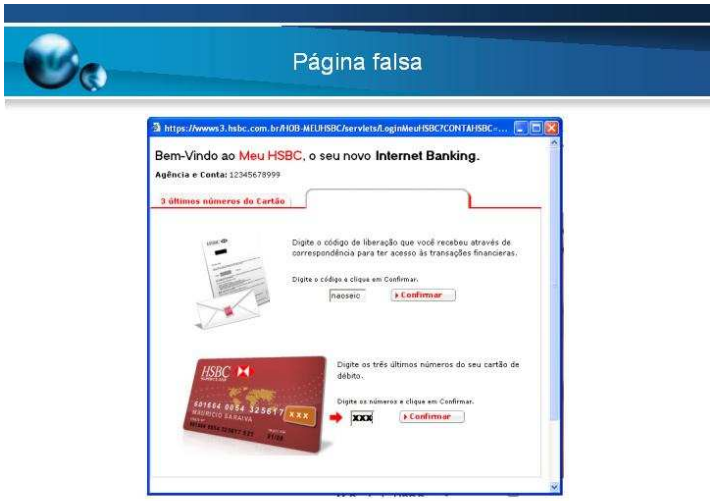




Quarto passo: "Teclado codificado. Utilize o teclado convencional". "Digite as letras referentes à sua senha do cartão de débito".

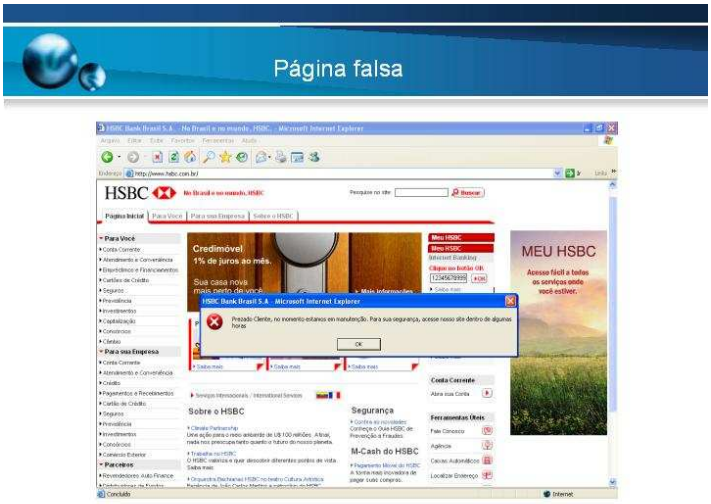
Aí acessa. "Digite o código de liberação que recebeu através da correspondência para ter acesso às transações". Nessa altura do campeonato, a pessoa pensa assim: o banco me ama, o banco me dá tanta atenção, sou um cliente especial.



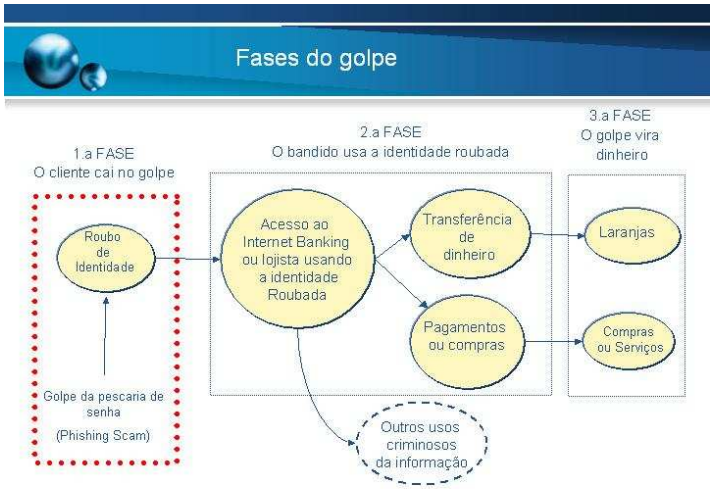


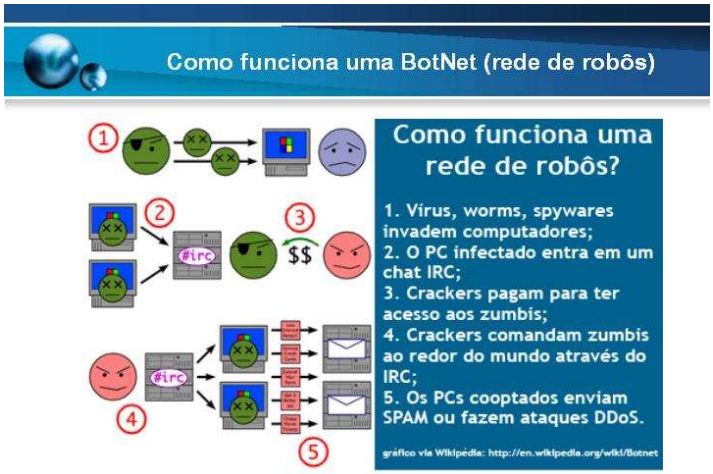
"Digite código de liberação que recebeu através da correspondência, digite os três últimos números do cartão de débito" – aquele código de segurança. Confirme sua senha do caixa automático. Para digitação das senhas alfabéticas, deve verificar quais caracteres representam as letras de sua senha". E por aí vai.

Depois que tudo foi liberado, está escrito assim: "Prezado cliente, no momento estamos em manutenção. Para sua segurança, acesse nosso site dentro de algumas horas". Quando a pessoa percebe, já retiraram todo dinheiro. Essa é uma prática muito comum.



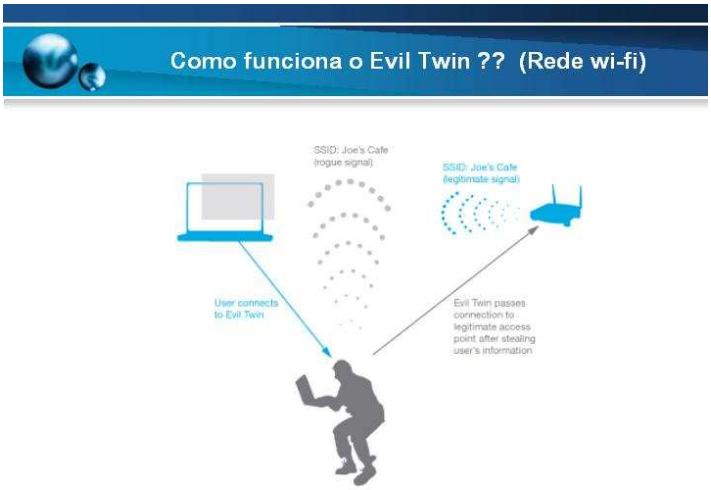
E aí vêm as fases do golpe.

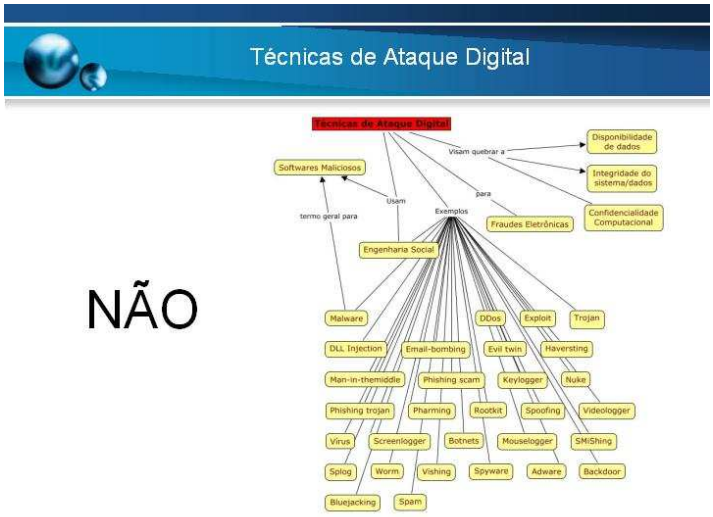




Aqui, o chamado *Denial of Service* (DoS).

Evil Twin, aquele da Guerra de Giz.





A interceptação.

NÃO

Observem esse jornal de 1999: "Assaltantes roubam sem sair de casa". Não é nem assalto e nem roubo.

Fraudes na Internet: exemplos

"Assaltantes roubam sem sair de casa: via internet"
(Jornal da Tarde, 8/9/1999)

Assaltantes roubam sem sair de casa. Via Internet

Fraudes na Internet: exemplos

Aí começaram a melhorar: "furtos *on line*". Eu tenho todos os fatos de crimes digitais que saíram na grande mídia.

"Aumento de furtos *on line* mobiliza polícia"
(Folha de S. Paulo, São Paulo, 9/9/1999, p. 3-8)

Polícia *Só em 3 DPs paulistanos, foram registrados 75 golpes de 3 tipos diferentes; bancos não crêem em quebra de sigilo*

Aumento de furtos on line mobiliza polícia

ALESSANDRO SILVA
da Reportagem Local

O crescimento dos golpes eletrônicos aplicados em contas correntes está preocupando a polícia de São Paulo. As delegacias já registram pelo menos três tipos diferentes de roubos eletrônicos – e todos eles vêm tendo aumento no número de queixas.

Nos últimos meses, só em três distritos policiais paulistanos foram registrados 43 golpes do cartão engolido seguido de saque, 21 queixas de pessoas lesadas em movimentação por telefone e 11 casos de furto on line.

Em Perdizes (zona sudoeste), a polícia recebe pelo menos uma queixa a cada três dias de cliente de banco que percebeu o sumiço do dinheiro que tinha na conta.

"Não conseguimos confirmar ainda se as retiradas foram por meio da Internet, principalmente porque esbarramos no sigilo bancário e na dificuldade de levantar informações", disse o delegado Edson Leal, do 23º DP.

Na região do Itaim Bibi (zona sudoeste de SP), o número de vítimas do furto on line quadruplicou nos últimos dois meses. Houve dois casos em julho, oito em agosto e um na primeira semana de setembro, com prejuízos que chegam a R$ 149,7 mil.

A polícia também investiga casos na Consolação.

"As queixas de furto pela Internet surgiram nos últimos meses e aumentaram de repente", disse o delegado do 15º DP, Orlando Basílio Ivanov.

O paulistano também está perdendo dinheiro pelo telefone. Pessoas que se identificam como funcionários do banco obtêm dados sigilosos de conta com a promessa de que o cliente vai ganhar cartão de crédito. De posse desses dados, desviam o dinheiro.

Outro golpe atinge os usuários do cartão, que acaba retido em caixas eletrônicos. O golpista, com a saída do cliente, retira o cartão e, como já tinha observado a senha, saca o dinheiro.

Sem estatísticas

O número de clientes lesados pode ser bem maior. O problema é que, embora tenha criado uma delegacia especializada em crimes eletrônicos, a polícia não tem estatísticas específicas sobre tais golpes. Os crimes aparecem nas estatísticas oficiais junto com outros tipos de estelionato.

A empresária Flávia S., que pediu para ter o nome preservado, teve prejuízo de R$ 30 mil.

Ela descobriu que seu dinheiro havia sido remetido pela Internet para contas em Goiânia, Fortaleza, São Luiz e até em São Paulo, dentro da rede do banco Itaú. A empresária utilizava o sistema "bankline", via Internet, para movimentar a conta. "Nem meu marido sabia qual era a minha senha." O dinheiro será devolvido pelo banco.

Esse aqui é da antiga ainda: "Cozinheiro que virou *hacker* roubou milhões de ricos e famosos" – inclusive do Spielberg.

Fraudes na Internet: exemplos

"Cozinheiro que virou hacker roubou milhões de ricos e famosos"
(Jornal da Tarde, Internacional, 21/3/2001, p. 9A)

Cozinheiro que virou hacker roubou milhões de ricos e famosos

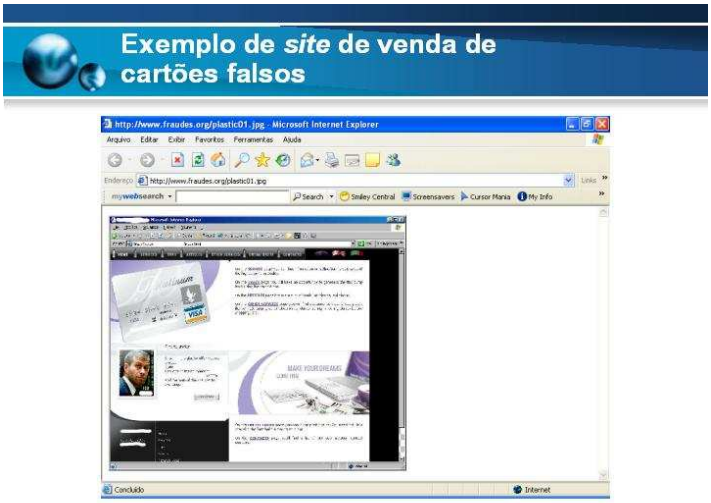
Esse caso é interessante, eu mantenho nos *slides*. Esses eram quadrilheiros da Zona Leste de São Paulo. "Clonadores viram alvos de seqüestro: banco muda senha de segurança".

Essas pessoas descobriram a "mina de ouro", e começaram a faturar em cima. O chefe dessa quadrilha comprou um helicóptero, de tanta grana. Eles foram oportunistas. Com a ajuda dos interessados, da Federação Brasileira de Bancos (Febrabam), eles foram identificados, presos, cumpriram parte da pena, alguns deles estão presos no Uruguai e outros em Portugal, porque fora do Brasil não tem aquela senha de segurança, alfanumérica, que troca a toda hora.

Mas o que é interessante é que suas mulheres começaram a ser sequestradas. O pessoal que roubava banco mesmo, sabendo que eles estavam faturando muito mais usando o golpe do cartão, começaram a sequestrar suas esposas.

Uns não foram reclamar, mas outros pagaram o resgate. Mas isso mostra é a migração do crime tradicional para o crime digital. As quadrilhas não são bobas, o pessoal está comprando cocaína daqui, ninguém mais liga para a Venezuela, Colômbia, para comprar; ninguém mais compra arma por telefone; é tudo pela internet.

Vejam: "Exemplo de *site* de cartões falsos".



Exemplo do "chupa-cabra". Não dá nem para falar; isso crime não é telemático, é informático, tinha uma câmara. Hoje as câmaras são menores. Quem encontrar isso aqui, mata, porque ninguém mais tem isso.

Exemplos de usos da internet para criminalidade organizada. Desde muito que isso acontece.

Exemplo de uso da Internet pela criminalidade organizada

"Golpe da pirâmide continua em alta"
(Diário Popular, Informática, 8/8/2000, p. 3)

Golpe da pirâmide continua em alta

Olhem: "Golpe de pirâmides continua em alta" – pela internet.

Programa de computador. É crime baixar *software* pela internet.

Lei n° 9.609/98: das infrações e das penalidades

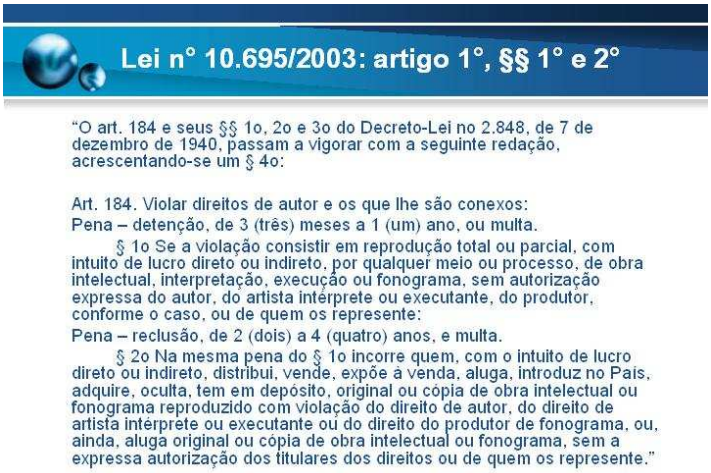
- Artigo 12:
  "Violar direitos de autor de programa de computador:
  - Pena - Detenção de seis meses a dois anos ou multa.
  - § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:
  - Pena - Reclusão de um a quatro anos e multa.
  - § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral.
  - § 3º Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:
  - I - quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;
  - II - quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.
  - § 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação."

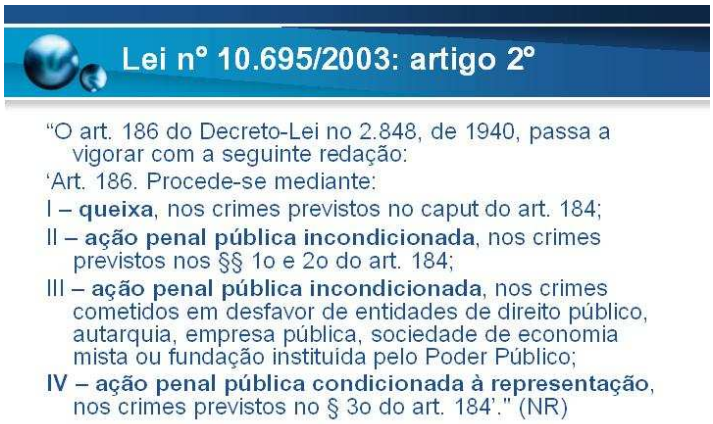
Propriedade intelectual

- Lei n° 10.695, de 1° de julho de 2003:
  "Altera e acresce parágrafo ao art. 184 e dá nova redação ao art. 186 do Decreto-Lei n° 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis n° 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o art. 185 do Decreto-Lei n° 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei n° 3.689, de 3 de outubro de 1941 – Código de Processo Penal."

Um exemplo de legislação sendo alterada pontualmente. Aqui a nova orientação, já de 2003.

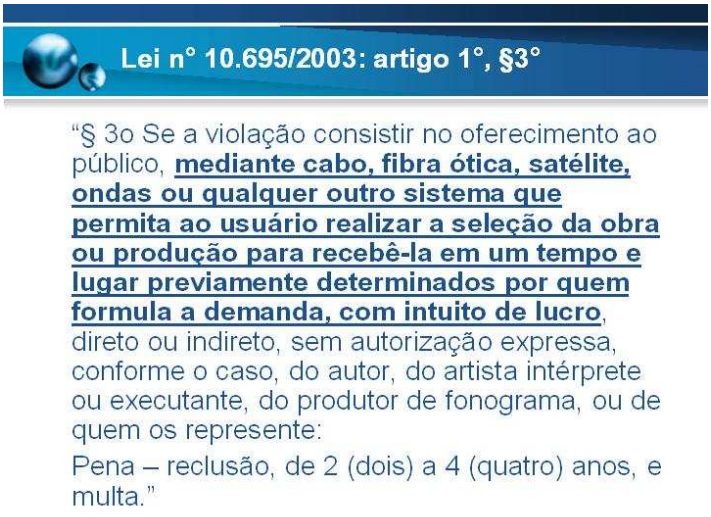
Mas o que nos interessa aqui não é o parágrafo primeiro ou o segundo; aliás, quem estiver estudando para concurso, se é que tem alguém que precisa estudar; se alguém perguntar quais os tipos de ação penal, vamos ao art. 184. Todas.



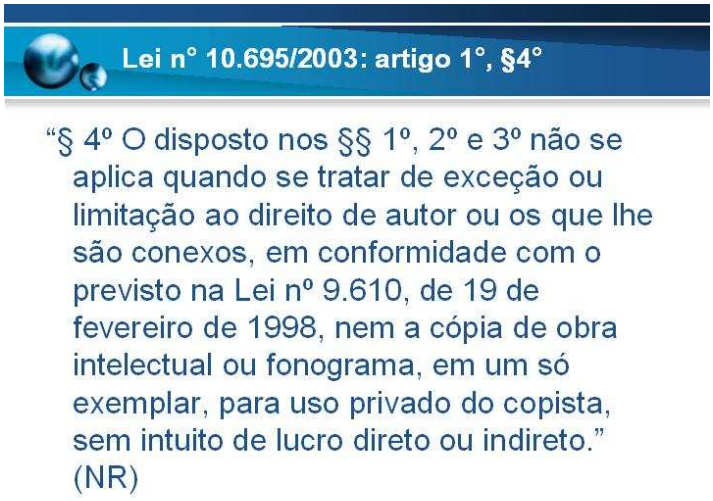


Ação penal privada, no **caput**; ação penal pública incondicionada, nos parágrafos primeiro e segundo; ação penal pública condicionada no terceiro. Todo tipo de ação penal encontra-se no art. 186. Quem for para o concurso, a resposta já está lá.

O que quer dizer é que esse projeto de lei foi construído para punir o "gato" de televisão. Mas agora estamos usando esse "gato" de televisão para a pirataria digital. Vejam: "se a violação consistir no oferecimento de público, mediante cabo, fibra ótica, satélite, ou qualquer outro sistema que permita ao usuário realizar a

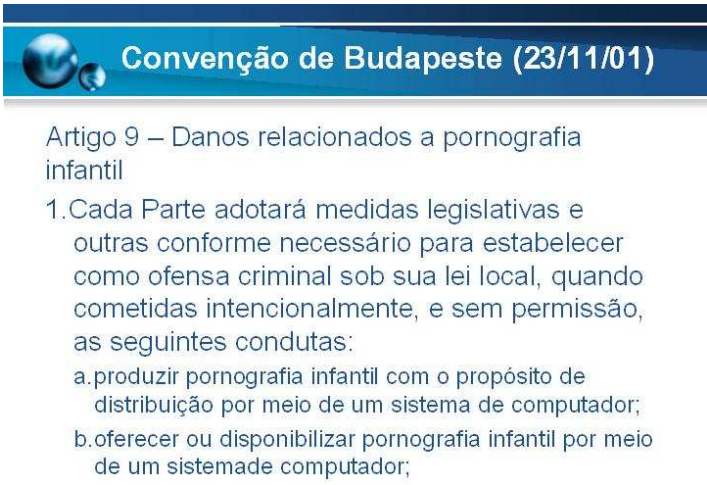


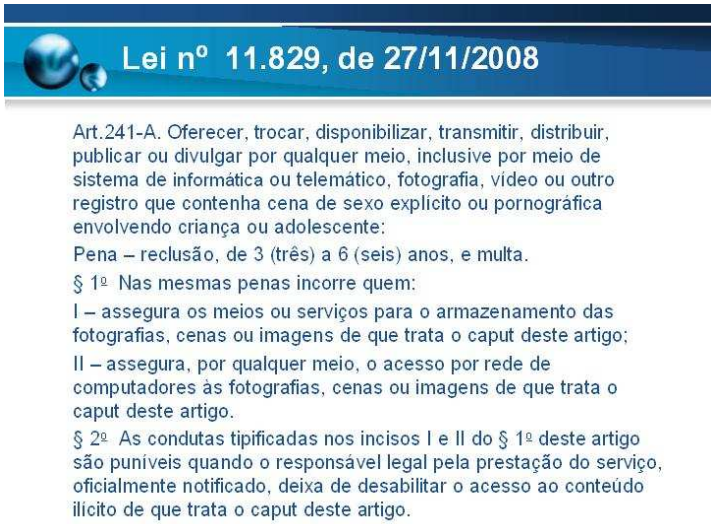
seleção da obra ou, por opção, para recebê-la em um tempo e lugar previamente determinados, com o intuito de lucro, direta ou indireto" Esse tipo está fácil de enquadrar a conduta. Mas é o caminho que temos para punir o pirata digital.



Não a cópia caseira, que tem aquela norma permissiva do parágrafo 4º. Perguntaram se baixar uma música para uso próprio, o parágrafo 4º está dizendo que não é conduta criminosa. Tem uma exceção. Esse é um exemplo de pirataria digital.

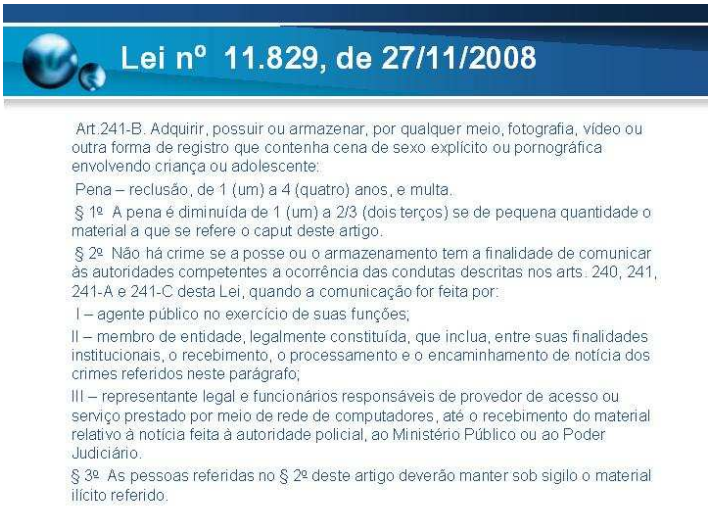
Outro caso. Pornografia infantil, a Convenção de Budapeste.





Agora a redação do art. 241-A, e aqui eu destaco o garantidor a que o professor se referiu: "oferecer, trocar, disponibilizar, transmitir, etc., os meios os serviços para armazenamento das fotografias, cenas ou imagens, assegura por qualquer meio acesso por redes de computador, as fotografias". O garantidor está aqui: "As condutas tipificadas nos incisos I e II do § 1 [...] são puníveis quando o responsável pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso". Ele se transforma em garantidor quando recebe uma notificação formal. Lá em São Paulo, o Ministério Público sustenta que essa notificação tem que partir no bojo de um devido processo legal ou procedimento interno, mas tem que ter portaria, autuação, registro, notadamente o inquérito policial, para que isso aconteça; caso contrário, não me parece que as garantias constitucionais seriam alcançadas.

Outro aspecto destacado pela lei, é que, se no art. 241-A, é *on line*, no art. 241-B, é a posse por qualquer meio. Aqui está a conduta da posse também.



E vem uma questão que os tribunais estão começando a diferenciar, a competência federal da competência estadual. O que é pornografia infantil estadual, e o que é pornografia federal. Está-se consolidando esse

entendimento, embora haja divergência nesse sentido, de que a pornografia federal é a do art. 241-A, que está na rede e tem tratado internacional, que o Brasil se submeteu a cumprir, e quando tem tratado internacional é a Justiça Federal, e é o Ministério Público Federal que tem que tratar. Então, existem normativas internacionais. Mas também porque são interestaduais, e sendo matéria interestadual, é uma regra da Constituição, quando o crime abarca mais o estado, é até uma questão utilitária, tem que ser mesmo. O que fica para a justiça estadual, o que temos recebido e não está tendo conflito negativo de competência? Na posse da máquina, quando se encontra na máquina, individualmente. E aí voltamos para aquela classificação inicial, temos um crime telemático, e telemático é o federal, e temos um crime informático, que é o estadual.

AUGUSTO EDUARDO DE SOUZA ROSSINI
Coordenador do CAOCrim – Centro de Apoio Operacional às Promotorias de Justiça Criminais
Tel. (11) – 3119 9924 e 3119 9925
E-mail: rossini@mp.sp.gov.br

E assim, só para deixá-los com raiva de mim, porque tenho vários assuntos para tratar, deixo o meu contato, e meu agradecimento a todos pela paciência de me ouvir.

Com isso, renovo meus agradecimentos. Espero que o tempo que perderam comigo não tenha sido jogado fora; espero que, assim com comecei pedindo a proteção de Deus, encerro também pedindo para que Deus nos ilumine todo dia, porque assim como Paulo disse na Epístola aos Romanos, capítulo treze, que a autoridade emana de Deus e em Nome dele é exercida. Cada um na sua parcela de poder tem essa missão divina, que é trazer a paz para a sociedade.

Obrigado e que Deus continue, repito, a nos proteger a todos. E que as injustiças, especialmente dos poderosos, possam ser punidas. Aliás, trago aqui o meu agradecimento, como cidadão brasileiro, pela coragem que esta Casa teve, através de seus ministros, no sentido de fazer com que a população brasileira volte a ter esperança e respeito pelas leis e pelas instituições sérias que construímos com tanto sacrifício.

Obrigado.

SEMINÁRIO DE DIREITO ELETRÔNICO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Iniciaremos, agora, a quarta e última palestra deste seminário. O Seminário de Direito Eletrônico é uma iniciativa do Centro de Ensino Superiores do Instituto dos Magistrados do Distrito Federal, Imag-DF, e do Superior Tribunal de Justiça.

Teremos, agora, a palestra com o tema *Perícia Forense*. Para ministrá-la, convidamos o palestrante, Dr. Ulysses Alves de Levy Machado.

O Dr. Ulysses Alves de Levy Machado é graduado em Direito, pela Universidade de Brasília (UnB); cursou *o Deming Program*, pela George Washington University; mestre em Direito Privado, pela Universidade Federal de Pernambuco; premiado no Conserpro, 2004, em nível nacional, com o trabalho *A Dimensão Jurídica do Software Livre e sua Aplicabilidade Como Forma de Equilíbrio na Construção de um Domínio Genuinamente Público*; é advogado do Serviço Federal de Processamento de Dados (SERPRO), onde exerceu a função de consultor jurídico pelo período de treze anos, atuando em matéria de Direito do Trabalho, Direito Administrativo, Direito em TI, Gestão de Segurança da Informação e Propriedade Intelectual; leciona na Centro Universitário do Distrito Federal (UDF), nas cadeiras de Especialização em Contratos, Direito Penal e Gestão da Segurança da Informação; especialista em Gestão da Segurança da Informação, pelo Departamento de Ciência da Computação da UnB; desenvolveu e publicou, no ano de 2008, o Portal DEVIR, Direito no Espaço Virtual, cujo endereço é www.devir.adv.br, e o *blog* DEVIR, atualizado no mesmo sítio.

Com a palavra o Dr. Ulysses Alves de Levy Machado.

PALESTRA VIII: PERÍCIA FORENSE

ULYSSES ALVES DE LEVY MACHADO
Especialista em Gestão da Segurança da Informação – UnB
Mestre em Direito Privado – Universidade de Pernambuco

Boa tarde a todos. Quero agradecer a esse convite, à possibilidade de estar aqui nesta casa, que é um templo nacional do Poder Jurisdicional, casa que vem enfrentando e construindo teses de suma importância para nós que atuamos na área do Direito no espaço virtual; agradeço a presença de todos até o final; fiquei surpreso, achei que com o andar da carruagem, a última palestra fosse ser prejudicada pela assistência, e fico feliz de ver que todos permaneceram. Prometo honrar essa generosidade e não aborrecê-los mais do que o necessário.

Na verdade, já contradizendo essa afirmação, preciso confessar a vocês que errei na mão. Preparei quarenta lâminas para essa palestra, mas juro por deus que não vou aborrecê-los com todas elas.

Como verão, esse material está disponível para os senhores. Cada lâmina dessas, que julgamos imprescindível no trato de forense computacional, foi devidamente anotada, com o conteúdo dessa lâmina. Então, não precisarão anotar, a menos que queiram fazê-lo, por hábito. Não precisarão anotar o que vamos falar, e o que eventualmente deixarmos de falar, estará registrado para que consultem.

Fora isso, independentemente dessa possibilidade, quero convidar a todos para visitar o site www.devir.adv.br e, nesse site deixei um *link* para o Imag, onde depositei tanto o material dessa palestra como diversos artigos e, em especial, uma monografia que escrevi para o curso de Gestão de Segurança da Informação, que se chama Delito e Resposta.

Procurei fazer essa monografia como uma forma de construir um oráculo de relacionamento entre o profissional do direito e o profissional de Tecnologia da Informação, uma tentativa de falarmos a mesma língua, que é uma tentativa antiga na minha profissão. Já tenho 25 anos de SERPRO, e ali tenho tido o prazer, a honra de trabalhar com os melhores *hackers* do cenário nacional, comparáveis a todos do cenário

internacional, com quem tive oportunidade de aprender e ter experiências muito nutritivas para o trato profissional do direito no espaço virtual.

Uso esse nome devir, senhores, porque significa o futuro chegando, e, ao mesmo tempo é uma sigla que remete a direito no espaço virtual, que é a melhor maneira de chamar isso que hoje chamamos direito eletrônico.

Direito eletrônico é uma impropriedade, tecnicamente falando o direito é o mesmo direito. Nós experimentamos até certa revolução no tempo, em função das novas tecnologias, mas o direito eletrônico não é substancialmente um direito diferente. Os princípios que regem o trato dessa matéria, como viram nas diversas palestras que me antecederam, é o mesmo direito tentando, como sempre, alcançar o inalcançável.

Vimos tentando, e uma dessas lutas foi mencionada agora, nas palestras anteriores, que é a luta do projeto de lei que faz a tipificação daqueles crimes, daqueles delitos, como são considerados, para aproveitar a correção do Professor Rossini. São delitos puros, cometidos no espaço virtual, para os quais não temos hoje tipificação, e, na verdade, esse projeto de lei seguiu em marcha trôpega, agora na Câmara dos Deputados, em função de um arrogante e agressivo *lobby* dos provedores de informática. Digo arrogante e agressivo, pode ficar parecendo uma figura de linguagem, um modo de falar, mas estou dizendo literalmente, em determinados momentos, sofremos agressão gratuita de determinados representantes do setor, que viam naquele projeto de lei uma ameaça ao paraíso fiscal em que vivem hoje. Os provedores têm uma situação tributária privilegiada, e apesar de ser um dos setores mais lucrativos – os senhores viram os mapas de crescimento, aqui apontados nas palestras anteriores – eles não querem ter o gasto, ter o custo, o insumo mínimo que é necessário para exercer qualquer atividade econômica, na civilização ocidental.

Quem fabrica armas, senhores, é obrigado a colocar número nas peças que fabrica, e essa providência não é barata, custa muito caro numerar um rifle Puma, calibre 38, numa série correta, aferível e

rastreável pela Polícia. Isso é caro, mas o setor tem que arcar com o ônus daquela atividade econômica a que se submetem.

Os provedores não querem isso, sob a bandeira bonita, poética de que é preciso preservar a liberdade na rede. Mas, olha, os campos de papoula, haxixe, nasceram selvagens. As papoulas nascem sem ninguém plantar, são naturais. Mas o uso que o filho do homem dá a essa papoula de haxixe, impõe o dever de regulamentar e regrar a atividade.

A internet nasceu livre, sim, mas as nossas crianças estão sendo impostas, o tráfico vem se utilizando da rede, os crimes vêm sendo cometidos, o direito de propriedade intelectual vem sendo aviltado, seja pela via criminosa, seja pela via política, como foi falado hoje de manhã pelo Professor Hildebrando Pontes Neto, de forma muito apropriada, na minha opinião.

E precisamos fazer alguma coisa. A comunidade internacional toda já começou a fazer alguma coisa. E nós estamos aqui brincando de liberdade. Que liberdade é essa que queremos? Os senhores acreditam que existe setenta por cento do tráfego entre a casa e o trabalho, hoje, que não seja filmado de alguma maneira, ou fotografado, ou monitorado? Cem por cento do meu trajeto de casa para o trabalho e do trabalho para casa, hoje, é filmado, gravado, monitorado, fotografado, e quero que seja assim, porque há pessoas desaparecendo nas ruas. Que liberdade é essa que queremos? É aquela liberdade dos seis meninos de Luziânia, que desapareceram da noite para o dia, deixando suas mães loucas? Aqui em Brasília, um homicídio foi resolvido a partir de uma câmera de gravação do Brasília Shopping. Os senhores devem se lembrar disso. E foi um carro da polícia, e nunca ninguém teria descoberto aquilo se não fosse a vida moderna, plantando as suas próprias soluções, para os próprios problemas.

"Forense computacional" – explico no início desse texto que deixo para os senhores – é um nome que a comunidade internacional inteira julga mais adequada para aquilo que vamos falar hoje, do que perícia

forense. A perícia forense é uma manifestação específica do que é a atividade de forense computacional.

A forense computacional, na verdade, nasce nas universidades norte-americanas, e do *Common Law* em geral, a partir do conceito de *forense science.* Nós não temos isso. Na Universidade George Washington, *forense science* é um departamento, tal qual o Departamento de Direito, e a matéria de criminologia que cursamos na George Washington University é ministrada em conjunto, uma *joint venture* entre o Departamento de Sociologia e o Departamento de *Forense Science. Forense Computers* I e II são duas matérias do curso de *Forense Science*. E, no Brasil, temos, por uma inversão historia da questão, as ciências forenses espalhadas – e mostro tal fato na estrutura da Universidade de Brasília da estrutura da Universidade Federal de Pernambuco –, entre diversas disciplinas. Temos em Biologia o estudo de forense biológica, tem, em Química, o estudo de Química Forense, e assim por diante, de forma não disciplinada; não existe um departamento de *forense science* em nossas universidades. E talvez isso venha a ser construído a partir da chegada desses *frameworks,* dos quais vou falar depois, que vêm disciplinando a atividade, pela via da qualidade e da auditoria; desde o Escândalo da Enron, parece que tudo de ruim, 11 de setembro, os atentados terroristas e os escândalos financeiros, acabam repercutindo como uma onde de coisa *pro bono,* ao longo do tempo.

O principal fator jurídico que decorreu do escândalo da Enron nos Estados Unidos, foi a conhecida Lei Sarbanes-Oxley[1] Essa lei tratou de disciplinar, nos Estados Unidos, e repercutiu no mundo inteiro, de forma também corretiva dos rumos, impondo rigores de qualidade e de regularidade em ciência da informação, de maneira geral. Dela resultaram vários modelos de qualidade, do tipo COBIT, do tipo ITIL, que são padrões ISO 9000[2]; quando falávamos, na ECO-92[3] , aquele *boom* da qualidade, a norma ISO foi regulamentada, no Brasil, pela Associação Brasileira de Normas Técnicas - ABNT[4], captada e aproveitada numa norma ABNT ISO, que disciplina qualidade e auditoria, e vamos falar sobre isso depois se tivermos tempo.

Por que começar falando de penal? Eu me senti muito tocado pelas falas do Professor Hildebrando, do Professor Rony Vainzof, ontem, e numa dessas falas, foi a respeito de licenciamento. Esse texto, e os textos da monografia que estão à disposição naquele site, são licenciados por uma licença específica, que não é *creative commons*. Ao repassarem esse texto para outras pessoas, peço que repassem as respectivas licenças, porque para esses produtos resolvi disciplinar um licenciamento de um tipo, e alguns textos desse *site*, que podem ser encontrados nos artigos e nos blogs, são textos licenciados por *creative commons*.

Compartilho perfeitamente do ponto de vista do Professor Hildebrando. Tem sido criada uma ditadura da ideia livre, como se quem utiliza de propriedade intelectual estivesse querendo "vampirizar" o

---

[1] Lei Sarbanes-Oxley (*Sarbanes-Oxley Act*) é uma lei americana, de 30 de julho de 2002. Motivada por escândalos financeiros coorporativos (dentre eles o da Enron, que acabou por afetar drasticamente a empresa de auditoria Arthur Andersen), essa lei foi redigida com o objetivo de evitar o esvaziamento dos investimentos financeiros e a fuga dos investidores causada pela aparente insegurança a respeito da governança adequada das empresas. Apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas.

[2] ISO **-** *International Organization for Standardization*. Organização não governamental que está presente, hoje, em cerca de 157 países, cuja função é promover a normatização de produtos e serviços, para que a qualidade dos mesmos seja permanentemente melhorada.

[3] ECO**-**92, Rio-92, II Conferência das Nações Unidas sobre o Meio Ambiente e Desenvolvimento, Rio de Janeiro, 1992

[4] Fundada em 1940, a Associação Brasileira de Normas Técnicas (ABNT) é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.

conhecimento na sociedade ocidental. Isso não é verdade. O artista, o autor, o cientista precisa comer, e a regra de propriedade intelectual que foi estabelecida desde o início dos tempos é a regra capitalista para esse tipo de negócio – foi assim que combinamos. E o mais grave que existe, nesse licenciamento, é uma confusão tola que se faz entre pirataria e software livre. Tem gente que imagina que software livre propugna a pirataria, ou incentiva a quebra unilateral de licenciamento, e isso não é verdade. Como propriedade intelectual é um dos bens passíveis de ser objeto de crime informático, e como a forense computacional tem por objeto também, vamos tratar, adiante, de propriedade intelectual. Sintam-se à vontade para interromper e perguntar, a qualquer momento. Isso já foi dito, mas quero reiterar, porque às vezes alguém pode ficar sem saber se pode interromper ou não. Podem gritar de lá, que eu paro de cá.

Esse é um conceito que formulei, **ad hoc**, para discutirmos, e, claro, é um conceito aberto. Não vamos fechar nada doutrinariamente, até porque quem sou eu para ficar ditando coisas desse tipo. Mas pensando em forense computacional, e no que ela representa hoje, fechei isso aqui, para a nossa discussão. Depois discutiremos alguns conceitos subsequentes.

"A análise de forense computacional é o empenho de conhecimentos técnicos voltados à investigação circunstancial ou ostensiva, de sistemas de informação visando, primeiro, a compreensão de um fato, e, segundo, ao esclarecimento de um incidente ou a avaliação da gravidade de seus efeitos".

A perícia forense a que estamos acostumados, o nosso cacoete processual brasileira, é apenas uma faceta da forense computacional. Eventualmente, a título de prova, o juiz se sentindo mal informado a respeito de um determinado tema, pode designar um perito judicial, para que as partes indiquem assistentes, promovam quesitos, e esses quesitos, após analisados, repudiados ou acatados, vão servir de escopo da atividade que aquele perito do juízo vai realizar, a partir daquela

circunstância que será examinada no caso concreto, daquela circunstância que vai ser examinada.

Explico que mudei o nome perícia forense para análise forense computacional porque análise forense computacional é mais que isso, a atividade **ad hoc** que o perito realiza quando é provocado pelo Poder Judiciário para produzir prova num determinado caso concreto é apenas uma faceta da forense computacional. Hoje, no mundo, os sistemas das grandes corporações, constroem, dentro das suas estruturas, uma coisa chamada gestão de segurança da informação. Nessa monografia que estou repassando a vocês, falamos em 220 páginas, a respeito de toda essa estrutura e de como ela funciona. A política de gestão de segurança da informação significa hoje a quebra da ingenuidade. Um dos artigos que deixei no subsítio Imag à sua disposição, é o artigo que fala exatamente da implantação – um caso real, fizemos a proposta de uma política de gestão de segurança da informação para o Governo de Angola, mais especificamente para o Ministério das Finanças daquele país – desse *case* de estudo que desenvolvemos aqui na Universidade de Brasília, UNB, no curso de Gestão de Segurança da Informação, como análise de caso. O que é preciso, vamos dizer assim, uma regra modelo, uma regra referência para implantar uma política de gestão de segurança da informação na organização.

Por que é importante, antes de pensar em forense da computação, pensar em uma política de gestão de segurança da informação na sua organização? Essa é uma organização, o Superior Tribunal de Justiça – STJ, que sem dúvida nenhuma mexe com tecnologia de ponta, tem à sua frente uma das missões mais difíceis do cenário nacional em termos de tecnologia da informação, que é implantar, o STJ assumiu, à frente do próprio Supremo Tribunal Federal, e à frente de todos os outros tribunais, a missão de transformar a prestação da tutela jurisdicional, do modo atômico, do modo físico para o modo eletrônico. E fazer isso não significa simplesmente "eletronicizar", como foi bem dito aqui pelo Professor Rony, ontem à tarde; não significa simplesmente mudar do papel para a tela do

computador, e vamos embora; não é isso, significa toda uma mudança de conduta e modo de pensar.

Sem uma política de gestão de segurança da informação, o STJ terá setenta por cento de dificuldade de cumprir essa missão, porque, como diz o meu orientador, o Professor João Gondim, nós, que estamos aqui nos defendendo do *hacker* maldito de fora do sistema, temos que adivinhar todas as formas de não errar. Alguém aqui é da área de tecnologia da informação? Os responsáveis pela área de Tecnologia de Informação têm que pensar em todas as cem mil possibilidades lembráveis, de não errar, enquanto uma pessoa do lado de fora, para pichar a página, um *script kid,* ou um *cracker* que queira realmente causar um dano, só precisa de um erro; tem todo tempo do mundo, uma lata de coca-cola, um monte de biscoito, de porcarias do lado de cá, e todo tempo do mundo para encontra um *back door,* para encontrar uma falha no sistema, só precisa disso, depois vai pensar na outra.

Quem gere segurança da informação não pode pensar assim. Se pensar está pensando com irresponsabilidade ou com muita falta de dinheiro. Quem gere segurança da informação tem que pensar em todos os erros, ou seja, estamos, eu e você, da Tecnologia da Informação, de todos nós, estamos em desvantagem.

É para isso que serve a forense computacional. Ela serve como um complemento, e verão nesses escritos. Não me aterei muito a esse, que é do Ajoy Ghosh, mas tanto um conceito quanto o outro são conceitos muito práticos, que não exprimem o que eles explicam, os modelos que analisam. Essa conceituação olha para a forense computacional com foco na coleta de evidências. Mas ao descrever como fazer isso, e como implantar a forma de tratar a forense computacional, vão muito além disso, e é nisso que nos pegamos.

Aquele nosso primeiro conceito menciona, vejam o círculo, que representa uma explanação mais complexa do que é aquilo que

chamamos o Ciclo PDCA [5]. Quando falamos no padrão adotado pela Austrália. Esse padrão australiano mostra exatamente qual é o ciclo de funcionamento da forense computacional, e da coleta de evidências.

Esse é o ciclo, que se olharem a ISO 9000, representa mais ou menos a mesma coisa. O Ciclo PDCA significa planejar, agir, controlar e corrigir. Ele vai do planejamento, passando pela ação até chegar ao aprendizado. Isso é forense computacional. A forense computacional significa implementar uma sistemática tal que gestores de TI, desenvolvedores, os fazedores de solução de um lado, auxiliados por auditoria, auxiliados pelos peritos forenses computacionais, pelo grupo de resposta a ataques, e pela auditoria de TI, vão atingir um sistema equilibrado. Invulnerável? Nunca invulnerável. O grande guru da tecnologia da informação, na minha opinião, foi Guimarães Rosa, que disse: viver é perigoso. Não existe um sistema de criptografia, conhecido, que possa garantir cem por cento de segurança. Quando estiverem buscando isso, esqueçam, pois não existe viver seguro, e muito menos em informática.

Mas é seguro, também, que essa falta de segurança vale de nós para eles. Mas única forma que temos de contra-agir, a partir de uma organização, é ter essa organização estruturada para poder responder a um determinado ataque.

Estruturei a palestra daqui para frente da seguinte forma: veremos forense computacional conceitualmente, vamos o que ela não é, vamos traçar um perfil do que é o agente de forense computacional, e veremos o perfil do atacante e o perfil dos ataques.

A forense computacional serve com possibilidade técnica de adentrar um determinado assunto colocado ali, um incidente ocorrido na organização. Alguém entrou na organização ORG e disponibilizou ao

[5] Ciclo PDCA (em inglês Plan, Do, Check e Action) é um ciclo de análise e melhoria, criado por Walter Shewhart, em meados da década de 20 e disseminado para o mundo por Deming. Essa ferramenta é de fundamental importância para a análise e melhoria dos processos organizacionais e para a eficácia do trabalho em equipe; ferramenta gerencial de tomada de decisões para garantir o alcance das metas necessárias à sobrevivência de uma organização, sendo composto das seguintes etapas: Planejar, executar, verificar, checar e agir corretamente.

concorrente DRIVE todo o portfólio de novos produtos que seria lançado para a coleção Primavera-Verão.

Vamos ter esse case em nossa cabeça, daqui até o final; vamos pensar nisso. Esse é um incidente modelo, um incidente padrão. Vamos vimos de tudo, tudo isso que o Professor falou na outra palestra. Por exemplo, *fishing,* inserção de vírus, injeção de código, *buffer over flow*, todos os ataques possíveis já vimos em matéria de forense computacional. Mas vamos usar esse padrão, que é um padrão-exemplo, ao qual aplicaremos os conceitos que vamos discutir aqui.

Alguém praticou, aparentemente, o crime de concorrência desleal em nossa empresa paradigma, e enviou ao concorrente, utilizando do próprio sistema da empresa ORG, ferramenta para fazer essa prática de concorrência desleal.

O Professor Augusto Rossini falou do *insider*. É aquele *hacker* interno, é o "cobra criada", aquele que a própria empresa produziu. Tudo leva a crer, nesse nosso exemplo paradigma, que esse *hacker* é um *insider,* porque precisa entrar naquela sala e fazer a remessa daquele material para o nosso concorrente.

Como vamos tratar esse incidente? Vamos pegar esse *case* e analisá-lo pensando em como a forense computacional trataria para fins de instruir aquele que é o que encomenda a investigação. Quem encomenda? O Professor Augusto Rossini, por exemplo, o investigador, o delegado de polícia, o juiz, eventualmente, ou na sua organização, já viram aqui no âmbito do STJ, alguma vez, um PDA, Processo Disciplinar Administrativo, às vezes precedido de uma comissão de sindicância. Já houve isso aqui no STJ, alguém tem conhecimento? Se alguém precisa de, julgando um PDA, apurar a certeza a respeito de quem foi o praticante daquela conduta delituosa, e ela envolve tecnologia da informação, é nesse momento que vai chamar o seu *expert* em forense computacional, que vai adentrar a essa nossa sala. Vamos fingir que o STJ é a organização ORG que criou a coleção Primavera-Verão que foi usurpada no nosso caso.

O meu orientador, Professor João Gondim diz assim: "Forense computacional é o segundo passo no processo de resposta a incidentes". Lá no SERPRO trabalho com uma organização chamada GRA – Grupo de Resposta a Ataques. Ela é coordenada pela Indiana, e tem lá uma coleção de malucos maravilhosos, o Glauco, o Viola, e outros doidos que trabalham até cinco horas da manhã, em regime de sobreaviso, com aquela latinha de coca-cola e o biscoito horrível aqui do lado também. Eles são pessoas dessa área aí, são loucos por isso, fazem por diversão, são encantados com esse processo.

Então, esses *hackers* internos são o nosso grupo de resposta a ataques, o GRA. As organizações usam esse nome, ou usam também Grupo de Resposta a Incidentes, ou usam o nome internacional dessa instituição, que é o C SIRTS. O mundo inteiro o C SIRTS é uma cadeia inter-organizacional, uma cadeia voluntária, eles se correspondem, trocam informações, promovem troca de conhecimento entre si. O SERPRO não inventou isso, e nem é o primeiro e nem o único, tem inúmeros GRAs no país inteiro.

O Professor João Gondim diz que "é o segundo passo no processo de resposta a incidentes". O GRA detectou o ataque, sua organização foi atacada, ele está vendo e viu que se consumou. Agora ele vai chamar o segundo passo, que é o expert em forense computacional, para ver quem foi que fez aquilo, porque fez aquilo; um investigador na polícia ou no PDA, onde quer que seja, vai querer saber isso, vai querer como, quando, porquê, de que forma; há possibilidade de se repetir, existe o risco de isso surgir de outra forma, outra forma não previsível?

E, em segundo, diz o Professor João Gondim que a atividade da forense computacional é "recuperar e analisar dados, da maneira mais imparcial e livre de distorções quanto possível para reconstruir os dados ou o que aconteceu a um sistema no passado".

O GRA é um grupo ativo, pode agir inclusive com certa agressividade. O perito forense computacional, não. Ele tem um perfil muito semelhante, sob o ponto de vista do conhecimento técnico, mas

não tem essa conduta. O forense computacional precisa produzir a prova mais objetiva possível, mas imparcial possível, e o mais completamente possível despida de juízo de valor. Veremos isso quando falarmos o laudo de conclusão do forense computacional, ao final.

Uma perícia computacional, uma análise forense computacional pode ser incidental ou corporativa. Pode ter na organização uma equipe de forense computacional, ou pode chamar uma organização que tenha essa equipe de *experts*, para atuar no seu problema, para atuar **ad hoc** em face do seu problema. E que problemas são esses? Incidente é o nome genérico, mas é possível instaurar uma análise de forense computacional em face de uma irregularidade – no fim temos o crime, temos o ilícito cível, temos a falta funcional, qualquer instabilidade, dano, lentidão, falso positivo é algo muito comum no trabalho de um GRA. O *hacker* está entrando, está forçando a porta de entrada, está tentando entrar, já passou pelo primeiro *firewall*. Pela forma de tentar acessar a rede, o GRA já sabe se é o *hacker*, o *cracker* para utilizar a nomenclatura do Professor Eduardo Rossini, ou se aquilo é a velhinha tentando, pela milionésima vez a senha, porque existe isso também. Estou dizendo a velhinha, porque nós, os anciãos, somos mais duros no trato com a coisa digital, com o teclado e com a apuração de senhas, mas normalmente é muito comum ter lá no final do perfil, a velhinha que diz meu filho fiquei tentando aqui, dei enter, enter e não conseguia. E era mesmo. O GRA sabe quando é a velhinha e sabe quando é o *hacker,* sabe se é o hacker *script kid,* sabe se é o *hacker lamer,* sabe se é o *cracker* profissional. Eles são capazes de traçar, informalmente, a conduta de cada um deles. Olha, isso aqui nunca vai ser um *hacker* guru. Nunca, guru não faz isso; isso é atrapalhado, a pessoa já entra chutando a porta, faz besteira, erra, vê que ele está errando. É completamente diferente. Então, pelo jeito que a pessoa tira o chapéu na porta de entrada, já sabem qual o perfil desse atacante.

E temos também a análise forense computacional corporativa. Qualquer uma das duas terá por objeto esse alvo de análise de investigação.

Nomenclatura acadêmica. Não tratarei desse tema, deixarei para lerem, sob pena de não falarmos coisas mais importantes.

Vimos conceitualmente o que é análise forense computacional, a que serve, e agora, para conceituar, por contraste, vamos ver o que ela não é, porque há uma série de atividades muito próximas de análise forense computacional, sobre as quais já falamos, que são a perícia judicial, a auditoria propriamente dita, a gestão de segurança da informação, que é ampla, abarca todos esses elementos, a perícia técnica propriamente dita, o exame de corpo de delito. De certa forma já falamos sobre alguns deles, dissemos que o perito judicial é uma parte do trabalho de forense computacional.

Auditoria e resposta a incidentes. O auditor funciona completamente diferente. Como é que funciona o auditor? A empresa tem problemas? Terá o auditor. Se a empresa não tem problema nenhum, terá o auditor, funcionando da mesma forma. O auditor de TI é um auditor como seu auditor interno. No Judiciário usamos mais a expressão corregedor, porque para a atividade judicial, que é o foco da sua organização, a corregedoria faz as vezes de auditoria da atividade fim, que é a atividade judicial. Mas nós, empresas públicas e empresas particulares, privadas, temos o auditor *in house,* e temos auditoria externa, que é contratada. Porque o auditor *in house* é contaminado pela própria organização. Todas as organizações, e isso tem suporte na Lei Sarbanes-Oxley, e em outras regras de mercado, o auditor *in house* faz o seu trabalho no seu ritmo, na sua periodicidade, mas periodicamente se chama também um auditor externo, que vem e avalia não só as contas da empresa por amostragem, mas também as do auditor. Auditoria de TI é a mesma coisa. O auditor de TI tem um plano de trabalho, auditor não funciona sem plano de trabalho.

Lembram quando falamos do perito judicial, que o perito funciona a partir dos quesitos que as partes formulam? O auditor também funciona por um escopo, mas o escopo dele é o plano de trabalho que realiza antes e por amostragem. Então, é muito comum ver o réu ou o prestador de

contas, o responsável quando o Tribunal de Contas da União (TCU) audita as contas, dizer, olha, não sei porque o TCU está mexendo nisso, nós já sofremos auditoria em 2008, 2009 e 2010, e nunca pegaram nada. É muito comum o cliente querer que façamos a sua defesa perante o Tribunal de Contas usando esse argumento de já ter havido a auditoria em anos anterios. Não, o perito funciona por amostragem. Ele escolheu aqui, jogou uma draga contábil, ou uma draga tecnológica, tirou uma amostra e examinou essa amostra. Se aprovou suas contas, aprovou olhando para esse universo restrito. Mas isso não significa que tudo esteja tudo bem, que não haja um *back door*, que tenha uma falha de rede.

O que o auditor de TI faz é exatamente o que o auditor de contas faz, examina por amostragem. No nosso caso, lá no SERPRO, a auditoria *in house* da empresa, tem também uma área de auditoria de TI. A auditoria de TI é uma área subordinada à auditoria geral; e eles atuam dessa forma.

Portanto, é uma atividade que não se confunde com a atividade de resposta a incidentes, sobre a qual já lhes falei. A pessoa de resposta a incidentes, não funciona assim, ele funciona entre o biscoito e a coca-cola, monitorando, com uma série de botões vermelhos, de luzes vermelhas para indicar a ele, olha, está "pegando" aqui, tem alguém tentando furar o *firewall*. Ele então vai responder, vai fazer ataques àquele incidente especificamente, ele é uma pessoa com um bastão de beisebol do lado de cá.

E o forense computacional é completamente diferente dos dois, funciona a partir de um incidente, sim, não necessariamente do leito derramado, mas funciona com um escopo delimitado pelas circunstâncias. O GRA funciona sem escopo nenhum, o que vier é dele, e o auditor funciona por um planejamento, que ele constrói. Faço essa diferenciação mais adianta.

Também já falamos de gestão de segurança da informação. Deixei o material para que leiam, e se interessarem-se, por favor, discutam

conosco; o blog está lá exatamente para isso, para tirarmos dúvidas, debatermos, aprendermos.

E o exame de corpo de delito é uma atividade muito específica dentro de forense computacional, dentro de perícia judicial, em hipótese alguma dentro de auditoria, não é isso, o auditor não faz exame de corpo de delito, o auditor não aponta isso, o auditor aponta desconformidades, não precisa ser necessariamente crime, não precisa ser necessariamente um delito, ou um ilícito cível; o auditor diz, por exemplo, que a forma de entradas não está compatível com o plano de segurança proposto inicialmente. É isso que o auditor fala. O perito diz, por exemplo, que, de fato, por tudo que foi examinado nos autos, é possível que o ataque formulado ao portão quatro tenha partido da submissão de *Jobs,* pelo IP 18.33.34 ou do IP 19.33.34, em função de que os *logs* examinados e as câmeras de vigilância, com as imagens que correspondem ao fato, permitiram concluir que, de fato, sem sombra de dúvida – pode até dizer assim, sem sombra de dúvida –, funcionou dessa e daquela forma. São linguagens até próximas, exigem até o mesmo tipo de conhecimento técnico, mas não se confundem no escopo e na metodologia que utilizam.

Citamos, então, sobre o que é forense computacional.

Internamente podemos falar de quatro espécies, em dois grupos separados, de forense computacional. Quando nos referimos a forense incidental ou a forense *post mortem,* o faço em relação àquela feita quando o "leite derramou". Então, em nossa sala, daquela organização ORG, já entramos e já verificamos que a Coleção Primavera-Verão foi vazada. Agora, vamos chamar a forense computacional para ver como foi isso. Será que foi mesmo? Foi. Não foi, não tem tráfego disso na rede, não constatamos isso. *Okay*, pode ter acabado aí. Mas isso é a forense *post mortem.* Mas muitas vezes a forense computacional é chamada para agir junto com o GRA. Estamos sendo atacados nos setores tais e tais da rede, o módulo tal da Receita está sendo violado. Foi violado? Não, está sendo, nesse momento agora. Então, vamos lá, enquanto o Grupo de Resposta a Ataques tenta debelar esse ataque, filtrar, controlar ou deixar

funcionar, porque se interromper o agressor pára e não o pegamos mais. Então, ou vai deixar funcionar, e eles sabem fazer isso, de modo controlado, até que seja identificado. E a forense computacional, por outro lado, vai tentar, em vida, no curso daquele incidente, identificar o modo, a autoria, a posição na rede, qual é o IP, de que *range* de IPs partiu aquele ataque, de que provedor, de que forma está tentando fazer isso. É possível que tenha ajudado interna? Essas são duas diferenciações básicas.

E abaixo ali, nunca mais vou usar essas cores, temos forense litúrgica e forense não-litúrgica. Muitas vezes, e isso foi muito comum nos anos oitenta e noventa, por exemplo, os bancos não queriam que os incidentes, as violações de segurança vazassem para o público, por razões óbvias, pois a atividade bancária vive muito de credibilidade. E que credibilidade teriam se aquele incidente vazasse? Então, às vezes a polícia era chamada, por uma razão ou por outra, mas o *Board* do banco decidia não oferecer queixa, arcando com os custos, e o banco pagava o cliente, assumia o prejuízo e tentava eliminar aquele *back door,* aquela porta aberta para a vulnerabilidade.

Isso mudou muito, do ano 2000 para cá os bancos têm mudado essa conduta. Eles têm feito muito aquela investigação prévia, da qual o Professor Rony falou, e às vezes, rejeitado, e imputa o prejuízo ao cliente o prejuízo. O Professor mostrou-nos um julgado em que o juiz diz – a decisão é até exagerada – que quem navega na rede sem um antivírus está assumindo o risco. Com esse raciocínio, o julgador eliminou a culpa e eliminou, com isso, a responsabilidade subjetiva, e afastou inclusive a objetiva mesmo, praticando imputou a culpa à vítima.

Os bancos têm passado a fazer isso, porque agora a relação custo-benefício faz com que valha à pena. Antigamente era um incidente, dez em um ano, isso era bobagem, saia na corrente do sistema, não tinha problema nenhum. Hoje, não, não é bem assim. Outro dia tivemos uma violação, na família, de conta bancária, um prejuízo de uns cinco mil, e o banco só pagou depois de muita investigação, e ameaçou muito não arcar

com o prejuízo. Só depois de ter checado que realmente foi uma falha de segurança do sistema, que não poderia ser atribuída à má utilização é que resolveu arcar com o prejuízo e pagou.

A forense litúrgica, essa é a diferenciação que importa, é aquela forense computacional cujo resultado poderá ser utilizado para pré-constituir prova e levar a juízo.

A qualidade da prova que a forense computacional precisa produzir é máxima. E veremos o que significa qualidade máxima em forense computacional. Se uma prova é constituída de modo a que possa ser contestada, e temos visto isso, numa falência, algo assim. Alguém citou um exemplo, o usuário pergunta onde estava esse HD, até o momento em que foi apresentado ao perito, como foi guardado, esse número foi modificado, temos o *Mac timing* dessa prova com data de julho, a coleta desse HD foi em janeiro, portanto mexeram nessa evidência; anulada a prova pericial, conforme a validade das outras provas testemunhas, documentais, o processo foi pelo ralo, o bom direito também foi junto, pelo ralo. Então, a forense computacional litúrgica precisa produzir uma prova inequívoca, com boa coleta, boa preservação dos dados, e vamos ver como isso se dá.

A forense não litúrgica é aquela do banco de antigamente, ou da própria organização, na qual a organização não quer litigar contra ninguém, mas apenas entender o que aconteceu para evitar que aconteça novamente. Nesses casos, não se quer laudo, não se quer que se fale com a imprensa, que a polícia seja chamada, não se quer nada. Como a organização é privada, não há o dever de apurar, mas de prestar contas ao *board,* que não quer saber de onde vem a água, só quer lavar a mão, e é preciso informar-lhe qual foi o resultado da investigação. Não se quer aquela furada, mas como aconteceu. A partir daí, o perito vai examinar informalmente, mostrar as evidências e explicar porque o fato aconteceu. Essa é a forense computacional não-litúrgica. A doutrina faz essa diferenciação em todos os manuais.

Perfil profissional de quem atua em forense computacional. Temos o perfil pessoal do profissional de forense computacional, e o perfil técnico. O que o perito idealmente tem que ser, sob o ponto de vista pessoal e profissional? Quando o SERPRO constituiu o atual grupo, na organização do SERPRO a forense computacional atua junto com o Grupo de Resposta a Ataques. Não considero que isso seja o ideal, é preciso, pela diferença de papel que ambos têm, que não tenham contato profissional íntimo, que não sejam colegas de trabalho. Por razões óbvias, porque quando auditamos ou investigamos um colega, a tendência, por mais honesto que seja, é levar em consideração os aspectos pessoais que conhece daquela pessoa. Então, não é o adequado. O SERPRO tem até peritos, analistas forenses computacionais fora do GRA, na área de gestão de segurança, e dentro do GRA. Eles são indistintamente chamados para compor aquela perícia, aquela equipe de análise forense computacional, conforme o caso. Muitas vezes temos, na equipe de forense computacional, um membro do GRA. Não é, como já disse, o ideal, mas até hoje não tivemos historicamente nenhum problema em relação a isso.

Quando essa equipe foi constituída, o que se fez foi uma investigação da vida pessoal e pregressa dessas pessoas, que se voluntariaram, eram voluntários a compor a equipe, e como voluntários já sabiam que seriam investigados sob esse ponto de vista. O foi investigado na vida dessas pessoas, que já eram empregados concursados, já tinham feito, inclusive, análise psicológica e psicotécnica, tudo que já sabemos que tem que ser feito para ser admitido em um concurso público. Eles foram chamados, eram voluntários, e tiveram suas vidas devassadas. Tem vício, bebe, tem distúrbios sexuais, já usou drogas, como é que foi na escola, qual foi o currículo, como é o histórico, tem dívidas, seu nome está no Serasa, já esteve no Serasa antes, tem dificuldades financeiras? Todos esses aspectos foram levadas em consideração para eleger discricionariamente aquela pessoa como apta a ocupar aquela atividade. Por que essa análise é feita com esse nível de profundidade? Porque é preciso que haja o menor risco possível, de a vida pessoal influenciar a

vida profissional daquela pessoa. E todos submeteram-se a tal procedimento de bom grado, até com exagerada violação da privacidade. Isso não foi inventado, foi copiado, é uma prática internacional, auditorias também são constituídas dessa forma, em investigações mais aprofundadas, mais detalhadas.

Para constituir uma equipe de resposta a ataques, ou uma equipe de forense constitucional ou de auditoria, é preciso ter certeza de que os componentes gozam de uma higidez econômica, psicológica, pessoal; ao serem chamados, já sabiam disso. Faremos uma chamada para o GRA, e haverá uma investigação na vida pessoal dos pretendentes. Quem estiver interessado em participar, já assina a adesão, sabendo da possibilidade de ser chamado e que terá a vida devassada. Portanto, não é violação de privacidade, a pessoa consente. E não houve nenhuma reclamação, todos brigaram muito para fazer parte, e expuseram voluntariamente os "esqueletos dos armários".

A finalidade é estar investigando um determinado ato, um determinado fato que está sendo apurado pela empresa, que talvez tenha sido praticado por agentes terceirizados da maior empresa de informática privada da América Latina, que tinha um determinado contrato com a empresa. Há desconfiança de que ou um *insider*, ou alguém dessa companhia pode ter criado, gerado um *back door*, ou feito um "tunelamento" da rede de segurança da empresa para fora, e vazado informações sigilosas da Receita Federal.

Se o empregado que fará a análise forense computacional ou a resposta a incidentes dessa natureza tem um problema de dívida, gosta de jogar, e às vezes o *bookmaker* é violento, e às vezes está na hora de pagar, e às vezes o funcionário, o diretor da companhia que está sendo investigada sabe disso, – não existe ingenuidade nesse mundo – chega para ele e diz que todos os seus problemas podem ser resolvidos... Existe a possibilidade de eliminar qualquer risco de corrupção? Não existe. Mesmo sendo feita toda essa análise, ainda pode prevaricar ou aceitar propina, suborno, ou qualquer tipo de corrupção.

Mas, na seleção, buscamos eliminar, essa é uma prática consensual, pelo perfil de seleção das pessoas que vão participar. É algo um pouco chocante, concordo, antes de fazer nos consultaram lá na COJUR três vezes. E se perguntar assim, assim, e se fizer assim e assim, posso exigir isso dessa forma? Pode, porque no edital de convocação deixou isso claro, foi explícito assim, mudamos aquela redação. Lembra aquela cláusula do edital que dizia isso? Alteramos para isso, e se é voluntário está sabendo daquilo.

Além do perfil pessoal, tem necessariamente que ter esses conhecimentos: técnicas de análise, bom raciocínio crítico. Em gestão de segurança da informação, aqui na UnB, chamamos o Professor Carnieli, de São Paulo, para dar um curso de vinte horas sobre raciocínio crítico, porque o laudo que é elaborado por um forense computacional precisa ser claro, não pode partir de premissas falsas e chegar a conclusões válidas. Não é possível. E é preciso ter treinamento para ceder à tentação, eventualmente, de ter efetividade no laudo computacional; precisa ter objetividade e raciocínio crítico e uma linguagem clara, para quem vai analisar. Não pode fazer o que nós, advogados, gostamos tanto de fazer, inventar palavras, usar latim. Não é essa a finalidade, o laudo pericial não tem esse escopo.

Temos aqui alguns exercícios.

No Brasil, a disciplina de análise de forense computacional é organizada em cursos de graduação unificados e em estrutura própria, com as correspondentes projeções em pós-graduação própria. Isso é verdade? Isso é uma coluna de verdadeiro ou falso. Como já falamos, não temos estruturação de forense computacional na academia brasileira, ela é dispersa.

A auditoria de sistemas inclui gestão de segurança de informação, e perícia computacional? Isso é falso, pois a auditoria de sistemas não inclui gestão de segurança da informação. Gestão de segurança da informação é que engloba, é preciso que se tenha auditoria, que se tenha

análise de forense computacional, um bom grupo de resposta a incidentes.

Esses exercícios estão à disposição, temos dez V ou F aqui, e dez V ou F lá no final. Se quiserem fazer e discutir, mandar por e-mail, fiquem à vontade. É uma forma de dirigir a leitura do material aí de quarenta páginas, que trouxe para aborrecê-los.

Agora, os *frameworks*. Nessa monografia que deixei à disposição lá no *site*, faço uma análise dos principais *frameworks*, que são o COBIT, o ITIL, a norma ISO 19000, e a 27 qualquer coisa. Uma trata de forense e a outra trata de gestão de segurança da informação e de algum outro que não estou lembrado agora.

Mas aqui, para a forense computacional, trouxe esses dois modelos. Esse *framework* tem por objeto a construção e toda uma metodologia de práticas, que, apesar de serem direcionadas para qualidade e responsabilidade ambiental, traduzem de forma importante a seriedade dos princípios que devem pautar a atuação de um auditor. Tais princípios vão informar não apenas as auditorias de segurança da informação, ordinárias, mas também a conduta de grupos de sindicância, processo disciplinar e de equipes de forense computacional. Ela carreia a adoção de princípios e de técnicas, práticas que têm que ser observadas para produzir-se uma análise correta dos fatos.

Explicamos aí com é parecido o PDCA[6] . O PDCA é uma ferramenta da norma ISO. A norma australiana adotou exatamente o PDCA, só que ao invés de quatro pontos, adotou esses seis. Mas eles representam exatamente o mesmo estágio cíclico de apuração. Por que é cíclico? Porque a partir das conclusões finais de uma análise computacional ou de uma auditoria é gerado aprendizado constante, numa espiral, de modo

[6] O ciclo PDCA, foi desenvolvido por Walter A. Shewart na década de 20, mas começou a ser conhecido como ciclo de Deming em 1950, por ter sido amplamente difundido por este. É uma técnica simples que visa o controle do processo, podendo ser usado de forma contínua para o gerenciamento das atividades de uma organização.

que não só os incidentes, mas as falhas de estrutura, relacionadas à infraestrutura técnica, ou ao meio ambiente, ou à atuação humana.

O nosso delito e resposta, que os senhores estão recebendo, foca, em matéria de segurança da informação, só a conduta humana, não enfoca incidentes do tipo terremoto ou incidentes técnicos do tipo blecaute geral da rede. Não, enfocamos gestão de segurança da informação só sob o ponto de vista humana, que é o que mais interessa ao Direito, e no qual estão localizadas noventa por cento das faltas, das falhas dos incidentes, em matéria e forense computacional.

Falamos do que é, do que não é forense computacional, com o que se relaciona, os *frameworks* gerais e o perfil do agente de forense computacional. Agora veremos os conceitos gerais, a partir de que ferramentas, de que conceitos os *frameworks*, as normas gerais, as boas práticas de forense computacional, exigem que uma Análise Forense Computacional (AFC) seja realizada, por meio de que ferramenta.

A primeira é o conceito de evidência. Evidência é todo fator agregado, para chegar a uma determinada conclusão final ou parcial, válida; aquilo que o investigador, que é o cliente da forense computacional precisa para fazer o trabalho dele. Evidência não é conclusão. O perito computacional, o analista de forense computacional, o perito judicial, quem quer que seja que faça algo parecido com forense computacional, não tem que chegar à conclusão. É muito frustrante quando mostramos para o cliente o laudo de um perito. O laudo é sempre uma coisa lacônica, e o cliente diz assim, mas ele não falou que teve aquele furo na rede. Calma, ele não tem que falar isso. O perito do juiz ou analista de forense computacional não conclui nada, tem que fazer um exercício constante de não roubar tarefas. Quem acusa é o Ministério Público, quem julga é o juiz, quem defende, sustenta teses, faz juízos de valor prévio para conduzir a convicção judicial, é o advogado. O analista de forense computacional não conclui, e, normalmente, quando o faz, invalida o laudo.

Os dois laudos periciais que tivemos oportunidade de ver anulados em processos que eram de nosso interesse, aliás, contra os nossos interesses, eram inválidos, porque o perito julgou, o perito quis colocar as palavras na boca do juiz, se envolveu com aquilo, se contaminou e, em função disso, cometeu outros erros, outras falhas que levaram à anulação daquele laudo. Não foi só pela conduta de convicção. Perito pode ter convicção? Pode, mas precisa ter aquela convicção – já assistiram ao *Star Trek*, lá não tem o Mr. Spok, aquele venusiano (sic) absolutamente frio, que não sorri, não chora, não sofre – do Mr. Spok, o analista computacional tem que ser aquilo, não pode se envolver, concluir, antecipar juízo de valor; quem tem que fazer isso é quem vai analisar para decidir no processo.

Achado já não é da linguagem de forense computacional, achado é coisa de auditor. Mas constantemente vemos auditores usando expressão "evidências", e analista forense computacional utilizando a expressão "achados". "Esse achado nos leva à convicção de que, não sei o que, não sei o que..." Não são expressões próprias, mas não inquina de forma alguma o laudo; apenas ocorre que as linguagem são diversas em função da finalidade, como vimos, são finalidades diversas. O analista de forense computacional não produz achados, porque o auditor, ao analisar, conclui. Quando o auditor diz "esse achado", já está dizendo, "olha, te peguei"; e o seu relatório final, que não é um laudo, é um relatório final, diz "encontramos isso, isso e isso; foi constatado, isso, isso e isso, e recomendamos, desde já, independentemente do julgamento das contas, que o administrador faça isso, isso e aquilo". Então, o auditor não é devedor de tamanha imparcialidade técnica, tem convicções, e as deita no papel, às vezes de forma dura, e às vezes mais que um juiz até, para determinadas tarefas o auditor tem mesmo a obrigação de concluir e julgar antecipadamente contas. Se o Tribunal de Contas vai ou não manter aquilo, aí é outra história, mas ele já antecipa.

Salvaguarda do ambiente de abordagem. Imagino que ainda estejam com aquela nossa imagem ali na cabeça, da sala de design da

nossa empresa ORG, onde alguém entrou pela manhã e constatou, pelo ambiente, que toda Coleção Primavera-Verão tinha sido distribuída para o concorrente. E deparamo-nos com aquela sala ali. Na convicção daquele gerente que viu, é o que chega mais cedo e se deparou com aquele quadro, o que vai fazer nessa nossa organização ORG, tão bem administrada, tão bem gerida, e que conta com uma política de gestão de segurança da informação? Vai convocar a equipe de análise forense computacional, porque parece que ali tem um aceno de crime. No mundo ideal isso funciona assim. No mundo prático, a primeira coisa que esse gerente faz é entrar e meter a mão no teclado, meter a mão no mouse, navegar pelas telas que estejam abertas ali, se certificar, ver que arquivos foram abertos. Quando faz isso, já meteu a mão no mouse, já pisou as impressões digitais que podiam haver ali, se haviam, se o *hacker* era uma *hacker* ingênuo ele deixou, e se não, limpou. E quando o analista forense computacional chega, tudo aquilo já está mexido.

Qual a percentagem de casos em que isso acontece? Na minha experiência pessoal, em cem por cento dos casos. Nunca chegamos e nos deparamos com uma cena de crime, entre aspas, ou potencialmente uma cena de crime, nunca nos deparamos com uma que não tivesse sido mexida. E uma vez falei isso para um Inspetor da Polícia Federal, e ele disse nem nós. Nunca, isso é impossível, todo mundo chega e fala, olha, tem alguma coisa estranha. Pronto, já era.

Lá nos primórdios da forense computacional, da *forense science*, um francês, Edmond Locard; criminologista, mas criminologista de uma época em que a criminologia não estava, com hoje é, tão associada à sociologia, ao pensamento abstrato. Não, era um analista forense computacional da época de Cesare Lombroso. Lombroso é aquela pessoa que analisava o cérebro das pessoas, e que constatou que o diâmetro do cérebro dos criminosos era normalmente maior, que normalmente eram mal encarados, normalmente eram pessoas feias; enfim, era muito organicista, muito pragmática a criminologia nesse momento. Mas o Edmond Locard não se imiscuía com esse tipo de discussão, era mais

ligado à Química. Então, ele examinou aquela atividade de forense computacional, e lançou o seguinte princípio: sempre que uma substância entra em contato com outra substância, existe, de uma para outra, troca de material. Isso é um princípio muito simples, mas que isso foi fundamental pela simplicidade. Pode parecer óbvio para nós, hoje, que já vimos filmes de detetive, e que se fala em impressão digital. Imaginem naquela época, se alguém iria pensar que quando alguém toca, deixa gordura da mão no formato único das impressões digitais, e com isso a pessoa pode ser identificada. Ninguém cogitava isso naquela época. Mais do que isso, independentemente de impressão digital, Edmond Locard disse que sempre que uma substância entra em contato com a outra, elas trocam material. É sempre? Foram ver, e constataram que é sempre. Sempre troca material. Isso valia para o bandido? Não, essa informação é útil para a polícia, porque a polícia, normalmente, chegava na cena do crime tateando em tudo, pisando e mexendo nas coisas, porque era assim que se chamava investigar naquele tempo, as coisas nem tinham nome ainda.

A partir desse princípio de Locard, o desenvolvimento de todas as técnicas de investigação, de forense computacional, passou a levar em consideração isso, e constataram que isso funcionava para tudo, seja para detectar impressões digitais, seja para se verificar que material foi utilizado em determinado homicídio, seja para investigar que tecido de roupa pertencia a quem, rastrear criminosos a partir daquele vestígio. Quer dizer, coisas impensáveis para a época passaram a ser feitas a partir desse princípio.

O mundo vem evoluindo, evoluindo, tivemos o surgimento do computador pessoal e da popularização do crime de informática. Onde é que entrar Locard? Estamos falando de crime digital, estamos falando de propriedade imaterial, estamos falando de propriedade intelectual, estamos falando de *bit*, não estamos falando de átomo. Os senhores consideram possível aplicar os princípios de Locard para essa faceta, essa feição tecnológica do crime? Todo mundo fica perplexo, mas prevalece a

Lei de Locard, até hoje, porque no tráfego de rede o que existe mais existe é troca de material virtual, o que mais existe é contato. Por onde trafegou esse pacote? É possível saber? É possível saber. E a maior quantidade de crimes cometidos, detectados e investigados com sucesso se deve à ignorância do próprio *hacker*, se deve ao fato de que ele ignora o quanto o tráfego daquele pacote venenoso que ele manda, ou daquela subtração que promove, como aquilo deixa rastro. Muitas vezes ele não sabe disso.

Existe um princípio chamado Lâmina de Valon, que nos diz para nunca atribuir à malícia aquilo que pode ser explicado pela simples estupidez. O *script kid*, aquele que sai atropelando, fazendo bobagem, pichando página, é mestre em deixar esse rastro, é muito difícil não deixar rastro.

A propósito, alguém me perguntou: "Professor, o senhor acha possível interceptar pacote de dados?" Olha, tem razão, no dia a dia não vemos isso, mas é perfeitamente possível. Se não fosse possível interceptar pacote de dados, não haveria necessidade nenhuma de tunelamento. Não é verdade? Haveria necessidade de fazermos um tunelamento VPN, se não existisse a possibilidade de alguma coisa ser interceptada? Nós criamos isso justamente pela possibilidade de interceptação. Só que no dia a dia pode não ser muito útil fazer isso, mas a segurança exige. Não tem um técnico do SERPRO que acesse a rede SERPRO, por exemplo, às vezes até do exterior, que não use o tunelamento por VPN, que é mais ou menos como se colocássemos um canudo imenso, da janela do nosso quarto até a empresa, e aí passássemos um cabo virtual por dentro dele, e a partir desse cabo emitíssemos determinado conteúdo. Por que isso é feito? Justamente pela possibilidade absolutamente clara, tranquila de se fazer isso. Quebra de senhas é uma bobagem.

Já aconteceu, por exemplo, num sábado à noite, me ligarem perguntando se podia ir até o Grupo de Resposta a Ataques, pois estava havendo um ataque de *fishing* no site da Receita Federal. Quando cheguei

lá o servidor estava com o dedo em cima do botão e disse: " – Estou esperando o senhor só para me dizer que pode". Eu perguntei: "– Pode o quê?" Ele respondeu: " – Quebrar a senha dessa caixa postal". Diante disso, replico: " – Calma, explique antes". " – É o seguinte: nós detectamos esse *fishing*, a pessoa recebeu um e-mail, abriu e viu lá, a Receita Federal informa que é preciso fazer o seu recadastramento, e, para isso, por segurança de rede, é preciso que dê a sua concordância para que enviemos uma senha pelo correio, o senhor concorda?" Ao que a pessoa respondeu que concordava; quando disse "concordo", o *fishing* fisgou o peixe; e aí instalou o emissor das senhas e das suas movimentações bancárias para um *e-mail* em Miami. De Miami, a pessoa abrir o conteúdo daquela correspondência, da Ucrânica; da Ucrânia, ele dava o comando e uma pessoa em Belfast fazia a emissão do comando e o saque do dinheiro dele para outra conta em Ubatuba. Em Ubatuba a pessoa dividia em tantas contas, até fazer a pulverização daquilo e faziam o saque do dinheiro.

Esse processo foi identificado: olha, tem uma conta em Miami; posso quebrar essa caixa postal, o e-mail da pessoa. Ele mandou do e-mail dele para um e-mail em Miami. Posso abrir a caixa postal? Eu disse: pode abrir, e quebramos o sigilo. Mas fez isso em um segundo, fez durante o tempo que me deslocava de casa até a empresa.

No primeiro dia, alguém estava dizendo que o Supremo Tribunal Federal, ao contrário do que o Superior Tribunal de Justiça fez, instalou um sistema de senhas e *password* para segurança do sistema eletrônico; o STJ não fez isso, usou certificação digital. Isso é seguro. Senha, senhores, é uma bobagem, é uma brincadeira de criança. A certificação digital funciona até hoje sem nenhum histórico de quebra, não tem nenhum histórico de violação. E não tem esse histórico de violação, porque funciona a partir de um conceito de segurança computacional. Segurança computacional significa o seguinte: é possível quebrar esse algoritmo mais complexo? É possível quebrar, mas a relação custo-benefício é baixa, inviável ou nula. Gastar-se-ia muito mais dinheiro que o

benefício possível de ser auferido com a quebra dessa chave. Por isso até hoje não tivemos nenhum negócio desses; e outra coisa, negócios muito valiosos e muito delicados não são feitos dessa forma, a pessoa pega um jato, viaja e fecha o negócio pessoalmente. Então, não tem, ainda, na rede, trafegando negócios, ainda que certificados digitalmente, em valores que tornem interessante fazer a quebra disso. Mas nada, no mundo, é seguro.

Locard, então, fez esse princípio que se associa à preservação do ambiente: quando chegar, chegue de mansinho, chegue educadamente, chame um perito forense computacional para que ele instrua como fazer isso. Ele vai fazer a abordagem daquela máquina de modo a preservar o que chamam de Cadeia de Custódia.

Cadeia de Custódia é exatamente a corrente de validade. Esse aqui é o HD da nossa empresa ORG? É. Vamos abordar essa máquina aqui. De que maneira essa máquina vai ser abordada? Para fazer a captação do HD, o processo tem que ser estancado? Tem que ser estancado. Mas, como, desligando a máquina, tirando da tomada, metendo o dedo no botão, fazendo CTrl-Alt-Del? Depende do tipo de sistema operacional que a organização usa. Lá no nosso delito e resposta, existe uma tabelinha de recomendações: se for Linux, desliga a máquina desse jeito; se for Windows, desliga daquele outro; se for OS MAC, desliga de outra maneira. E ele vai fazer a abordagem dessa máquina fazendo o que todo mundo chama de cópia Bit a Bit. Na realidade, aprendi recentemente que não existe a possibilidade de fazer cópia Bit a Bit, o que é feito é cópia de pacote a pacote. Do que estamos falando? Se fizer uma cópia, simplesmente, do seu HD, Ctrl-C, Ctrl-V de um lado para o outro, estará trazendo e apagando um monte de informações. Perícia computacional não pode ser feita em material recolhido dessa forma, tem que ser feito em material recolhido de forma profissional, com preservação da cadeia de custódia, que significa dizer que ninguém mexeu nisso, peguei o HD dessa máquina, na presença das pessoas, documentado de forma fotográfica e fiz uma cópia pacote a pacote, para esse HD; e fiz essa cópia

assinando isso com um algoritmo CHAO I ou MD5, que são os mais comuns.

Então, qualquer alteração que alguém faça nesse HD será feita de forma evidente, vai aparentar, não vai fazer sem que fique denunciado. O algoritmo faz com que essa coleta seja integral e não tenha perda dos dados. Isso vai ser feito em duas cópias, entregue uma cópia para o responsável do setor, e a outra vai levar para analisar. Existe toda uma técnica de coleta desse material, para que se preserve no seu relatório final a sua cadeia de custódia. A evidência coletada aqui é toda hígida, toda saudável, de forma documentada.

Vou saltar perfil do atacante, porque darei a matéria como lida, como eles fazem no Legislativo, uma vez que o Professor Rossini já desfiou um rol bem completo de perfis de atacante, mas verão esse perfil, também, no delito e resposta, que estão recebendo de graça, leiam, façam sua crítica, dêem um *feed back*.

Tipos de crimes, tipos de ataques. Há aí uma série de classificações, além daquelas que o professor disse. Essas são classificações muito interessantes, classificações de crimes como manipulações de dados, falsificações de dados, uso ilícito. O Ulrich Sieber faz uma classificação quadrúpla, para ele existem crimes de manipulação de dados, espionagem e pirataria, sabotagem de dados e acesso não autorizado. Já Jean Pradel diz que para obter dinheiro e informação – que penso ser uma classificação muito simplista. Existem inúmeras classificações. Mas aqui estamos falando de classificação de crimes, e para a forense computacional não interessa essa classificação de forma tão severa, tão importante.

Os tipos de ataque. Esse é um conceito de incidente, sobre o qual já falamos.

E aqui trago uma descrição de diversos ataques. Esse é um ataque de vírus. Além do texto que está lá embaixo, temos aqui um quadro, a partir de 1988, de todos os eventos mais interessantes, envolvendo ataques por vírus. Temos os famosos Chernobyl, I Love You, além de um

vírus que ganhou o nome da maravilhosa Ana Kurnikova. São vários eventos importantes.

O vírus é isso, essa coisa que entra na sua máquina, para te "lascar", para criar problema, lentidão, confusão; já o *trojan*, que vem na tela seguinte, traz coisas mais operacionais, do tipo mandar mensagem para os seus amigos todos, criar vícios de identidade, lentidão também.

Spyware é algo mais parecido com o *fishing* que já descrevemos. Alguém citou aqui que se separou da mulher, e deixou lá um *spyware* que repassava a ele toda a cadeia de transações que a mulher fazia.

Os *botnets*, que são práticas de escravidão coletiva. Esse é um ataque muito poderoso, pois gera o controle de inúmeras máquinas, de gente que nem conhece, simplesmente espalha o mecanismo na rede e essas máquinas ficam todas ligadas e sob o seu controle. Ao utilizar a estação de trabalho, não se sabe que isso está acontecendo, pode-se detectar eventualmente alguma lentidão, mas sua máquina está sendo usada como um zumbi para atacar, vamos dizer, as Lojas Americanas. Ou seja, a pessoa cria centenas de máquinas zumbis, e todas elas fazem ataques simples, apenas de obstrução de informações, que chamam *de denial of service*, simplesmente paralisando a organização.

O *spoofing* é uma prática muito utilizada para fazer aquilo que disse ao Professor Rossini. Significa se mascarar, se disfarçar. É uma das formas de se praticar o que se chama *man in the middle,* ou seja, uma pessoa do meio, que se interpõe entre duas pessoas, e faz o papel, simula a ação daquele destinatário ou daquele remetente.

O *smurfing*, é gerar, através de pacotes, um ataque que é de negação de serviço também; joga um pacote ICMP, como se fosse uma entidade na rede. Não vem o pacote IP? É o seu pacote IP, que trafega com suas informações na rede. Esse pacote ICMP entra num determinado sistema e diz assim: tem alguém aí? Tem alguém aí? Tem alguém aí? A máquina é burra, é feita para dizer sim. Toda vez que se pergunta tem alguém aí, a máquina passa a responder e a fazer mais nada, a não ser dizer sim, sim, sim. É quando está tudo parado, está sendo "smurfado". O

nome vem daqueles bonecos, os *smurfies,* que atacavam o vilão da história, eram muitos e muito "formiguentos". Os *smurfies* são isso, e isso deu o nome a esse pacote.

O *buffer overflow* significa basicamente entulhar alguma coisa de informação. Também é um ataque do tipo negação de serviço. A organização simplesmente para.

Existem inúmeras outras formas de ataque. No livro faço um comentário mais detalhado de cada uma delas. Para as pessoas de TI, isso é um tédio. Pulem, rasguem, joguem fora, não leiam isso. Mas para quem e leigo e se interessar talvez seja útil.

Quero que leiam isso. O Professor Rossini falou de engenharia social. Como o meu livro trata de conduta humana, é uma parte muito importante. Sugiro que não só leiam, mas vejam esse vídeo que estou sugerindo – esse *link* os levará ao *Youtube*, e lá existe uma aulinha básica a respeito de engenharia social.

Tem várias. Se entrarem no *Youtube* e colocaram engenharia social, vão compreender que algumas pessoas na humanidade já descobriram que por mais que o sistema seja perfeito, no meio deles tem um elemento chamado pessoa. Outro dia vi um vigarista dizendo isso num filme: eu não queria enganar as pessoas, mas todo mundo que encontro me pede, diz: engana-me.

Uma grande amiga, que tem três doutorados, super inteligente, caiu num conto de cigana e, depois que a moça foi embora, disse: "Meu Deus, com fiz isso! Sabia que estava sendo enganada, e fui". As pessoas já descobriram isso. Trinta por cento da humanidade já descobriu que é fácil: a gente pede às pessoas para nos enganarem. E engenharia social, partindo desse princípio, é uma prática, uma conduta, chama-se engenharia, mas não é engenharia coisa nenhuma, não é uma ciência, são práticas muito comuns, que são utilizadas para se beneficiar dos *back doors* que qualquer sistema oferece. E o analista de gestão de segurança precisa estar atento a isso.

Chegando ao relatório final, ele traz uma série de requisitos, mas basicamente ele deve seguir a estrutura que segue um parecer, que segue uma monografia, que segue uma sentença. Qual é essa estrutura? Essa estrutura é a estrutura do velho e bom silogismo: tese, antítese e síntese, relato, discussão, conclusão. Tem que ter essa estrutura e esse fecho.

Isso vale para qualquer análise de forense computacional? Não vale para qualquer análise de forense computacional. A análise forense não litúrgica não precisa seguir essa estrutura, mas se o laudo pericial precisa constituir previamente ou como prova no curso do processo tem que seguir essa estrutura basicamente, tem que ser claro, científico e se pautar pelo raciocínio crítico.

Aí tem o exercício dois. Façam e mandem-me.

Abaixo está a bibliografia básica.

Muito obrigado pela sua atenção.

ENCERRAMENTO

ROOSEVELT SILVA DE FARIAS
Mestre de Cerimônias

Senhoras e Senhores, chegamos ao final do Seminário de Direito Eletrônico.

Agradecemos a presença de todos e convidamo-los para um pequeno lanche que será servido no hall de saída.

Desejamos a todos uma boa noite e um ótimo final de semana.